Bell inequalities, classical cryptography and fractals

E. Shchukin*
Arbeitsgruppe Quantenoptik, Institut für Physik, Universität Rostock, D-18051 Rostock, Germany

The relation between the boolean functions and Bell inequalities for qubits is analyzed. The connection between the maximal quantum violation of a Bell inequality and the nonlinearity of the corresponding boolean function is discussed. A visualization scheme of boolean functions is proposed. An attempt to classify Bell inequalities for qubits is made, a weaker result (classification with respect to Jevons group) is obtained. The fractal structure of the classification is shown. All constructs are illustrated by *Mathematica* code.

I. INTRODUCTION

In their famous paper [1] Einstein, Podolsky and Rosen (EPR) suggested a Gedankenexperiment which, as they believed, must prove the incompleteness of quantum mechanics. An interesting analysis of this problem was given by Bohr [2]. Some progress was achieved by Bell [3]. He showed that under assumption of the EPR arguments some inequalities must be fulfilled. If Bohr's arguments are correct then these inequalities can be violated. It was only in 1980 when the Bohr's arguments were experimentally verified [4, 5, 6, 7, 8]. Now the arguments by EPR are considered to be incorrect, but nevertheless it is the work [1] that initiated the discussion of basics of quantum mechanics.

In this work I analyze the connection between the boolean functions theory and Bell inequalities for multi-qubit systems (which were obtained in [9]). Surprisingly enough, in many aspects Bell inequalities theory is analogous to the combinatorial problems of computer logic circuits design developed a year earlier then the Bell's work [3] appeared. There is also a relation between Bell inequalities and applications of boolean functions theory to classical cryptography. For example, classification of Bell inequalities discussed in [9] is closely connected to the Jevons group, studied in [10, 11], and the maximal quantum violation of a given Bell inequality is connected to the nonlinearity of the corresponding boolean function. I made an attempt to clarify these connections. But there are still many open questions, both combinatorial (like classification of Bell inequalities with respect to the group $\mathcal{G}_n$) and analytical (like calculation of the maximal quantum violation v_f). Another interesting problem is the connection between the maximal quantum violation and the uncertainty relation for boolean functions. In this work it is shown that the Bell inequalities whose maximal quantum violation is the largest (Mermin inequalities), minimize this uncertainty relation.

All mathematical constructions discussed in the text are illustrated with *Mathematica*. I choose *Mathematica* since it has an extremely flexible and unified programming language and a very rich set of built-in mathematical functions. Due to this it is possible to present the algorithms illustrating the discussed quantities in a very compact form. Using *Mathematica*, it is possible to code all the illustrating examples using high-level constructions, avoiding worrying about low-level programming details which have nothing to do with the problem under study. I do not pretend to give the most effective *Mathematica* code for calculating different features of boolean functions, my goal is to present a compact and ready-to-use working code. All the examples can be typed in and run provided that they are entered to *Mathematica* in the given order. I also presented the *C* source code for the fast Walsh-Hadamard transform and a way to turn it into an executable program which can be used in *Mathematica*.

II. BOOLEAN FUNCTIONS

The Bell inequalities for a multi-qubit system, which were obtained in [3], are closely connected with boolean functions theory. There is a natural one-to-one correspondence between the set of all $B_n = 2^{2^n}$ boolean functions of n boolean variables and the set of Bell inequalities for n-qubits. In this section I give a short overview of the notions and results of the boolean functions theory which are needed for applications to Bell inequalities. The most important notion discussed in this section is the Walsh-Hadamar transform, which turns out to be the coefficients of the Bell inequality corresponding to a given boolean function.

Here I also introduce a visualization technique of boolean functions which is useful to graphically represent different classes of boolean functions. This approach is based on the fact that for all n the number of boolean functions of n variables is a square (in fact, $B_n = B_{n-1}^2$), so that one can associate the boolean functions with the cells of a $B_{n-1} \times B_{n-1}$ array. Briefly speaking, this is done numerating boolean functions with integers, interpreting the vectors of their values as binary decompositions and then using division modulo B_{n-1}. In this section I visualize boolean functions with respect to their degree and uncertainty. In both cases the pictures show some kind of fractal behavior.

*Electronic address: evgeny.shchukin@gmail.com

A. Boolean vectors

Let $\mathbf{Z}_2 = \mathbf{Z}/2\mathbf{Z}$ be the finite field with two elements $\mathbf{Z}_2 = \{0, 1\}$. The sum and the product of elements $a, b \in \mathbf{Z}_2$ are denoted as $a \oplus b$ and ab respectively. The product of n copies of $\mathbf{Z}_2$ we denote as $V_n = \mathbf{Z}_2^n$ and refer to its elements as (n-dimensional) boolean vectors. It is clear that $|V_n| = 2^n$. The notation $\langle \mathbf{x}, \mathbf{y} \rangle$ is used for the scalar product of two boolean vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$:

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n. \tag{1}$$

There is a natural one-to-one correspondence b_n between the set V_n and the set $\mathcal{B}_n = \{0, \ldots, 2^n - 1\}$:

$$b_n : V_n \ni \mathbf{x} = (x_1, \ldots, x_n) \to x = \sum_{i=1}^{n} x_i 2^{n-i} \in \mathcal{B}_n. \tag{2}$$

In other words, the boolean vector $\mathbf{x}$ corresponds to the integer x whose binary representation is given by $\mathbf{x}$. The most significant bit in the binary decomposition of x is the first component of $\mathbf{x}$ and the least significant bit is the last component. The correspondence b_n is natural in the following sense. For an integer $m < n$ the set V_m can be identified with a subset of V_n by padding m-dimensional boolean vectors on the left to extend them to n dimensions. Then the diagram

$$\begin{array}{ccc} V_m & \xrightarrow{b_m} & \mathcal{B}_m \\ \cap & & \cap \\ V_n & \xrightarrow{b_n} & \mathcal{B}_n \end{array} \tag{3}$$

is commutative. This means that one can apply b_n to m-dimensional boolean vectors with $m < n$. The correspondence b_n is illustrated by Table I.

$\mathbf{x}$	$b_n(\mathbf{x})$	$m=1$	$m=2$	$m=3$
$(0,0,\ldots,0,0,0)$	0	$b_1(0)$	$b_2(0,0)$	$b_3(0,0,0)$
$(0,0,\ldots,0,0,1)$	1	$b_1(1)$	$b_2(0,1)$	$b_3(0,0,1)$
$(0,0,\ldots,0,1,0)$	2		$b_2(1,0)$	$b_3(0,1,0)$
$(0,0,\ldots,0,1,1)$	3		$b_2(1,1)$	$b_3(0,1,1)$
$(0,0,\ldots,1,0,0)$	4			$b_3(1,0,0)$
$\ldots$	$\ldots$			$\ldots$
$(0,0,\ldots,1,1,1)$	7			$b_3(1,1,1)$
$\ldots$	$\ldots$			
$(1,0,\ldots,0,0,0)$	2^{n-1}			
$\ldots$	$\ldots$			
$(1,1,\ldots,1,1,1)$	$2^n - 1$			

TABLE I: The correspondence b_n between boolean vectors $\mathbf{x} \in V_n$ and integer numbers $x \in \mathcal{B}_n$.

The set V_n can be ordered in many ways. I use the lexicographical order: for $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ the notation $\mathbf{x} <^{\text{lex}} \mathbf{y}$ means that there is k, $1 \leqslant k \leqslant n$, such that $x_i = y_i$ for $i = 1, \ldots, k-1$, but $x_k = 0$ and $y_k = 1$. Here 0 and 1 are elements of $\mathbf{Z}_2$, but if one considers them to be integers, the same can be shorter formulated as: $\mathbf{x} <^{\text{lex}} \mathbf{y}$ if and only if the first non-zero difference $y_1 - x_1, \ldots, y_n - x_n$ is positive. Since

$$\sum_{i=1}^{k-1} 2^i = 2^k - 1 < 2^k, \tag{4}$$

it is clear that $\mathbf{x} <^{\text{lex}} \mathbf{y}$ if and only if $x < y$, where $x = b_n(\mathbf{x})$ and $y = b_n(\mathbf{y})$. This means that b_n preserves the order:

$$(V_n, <^{\text{lex}}) \simeq (\mathcal{B}_n, <). \tag{5}$$

There are two very important functions on V_n: Hemming weight $\text{wt}(\mathbf{x})$ and Hemming distance $d(\mathbf{x}, \mathbf{y})$. The Hemming weight $\text{wt}(\mathbf{x})$ of a boolean vector $\mathbf{x} \in V_n$ is defined to be the number of non-zero components of $\mathbf{x}$. The Hemming distance between two boolean vectors $\mathbf{x}, \mathbf{y} \in V_n$ is the number of positions where components of $\mathbf{x}$ and $\mathbf{y}$ differ. It is clear that the distance can be expressed in terms of the Hemming weight as $d(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} \oplus \mathbf{y})$. Both the notions play an important role in different applications of boolean functions theory.

B. Boolean functions

A boolean function $f(\mathbf{x}) \equiv f(x_1, \ldots, x_n)$ of n boolean variables is a map $f : V_n \to \mathbf{Z}_2$. The set of all boolean functions of n boolean variables we denote as F_n. There is a one-to-one correspondence between F_n and V_{2^n}:

$$F_n \ni f \to \big(f(b_n^{-1}(2^n - 1)), \ldots, f(b_n^{-1}(0))\big) \in V_{2^n}. \tag{6}$$

Due to this we have $|F_n| = 2^{2^n}$.

Any boolean function $f \in \mathcal{F}_n$ can be represented in the following form:

$$f(\mathbf{x}) = \bigoplus_{\mathbf{y} \in V_n} g_f(\mathbf{y}) \mathbf{x}^{\mathbf{y}}, \tag{7}$$

where $g_f \in F_n$ and $\mathbf{x}^{\mathbf{y}} = x_1^{y_1} \ldots x_n^{y_n}$ (with $0^0 = 1$) or in the equivalent form as

$$f(\mathbf{x}) = c_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{1 \leqslant i_1 < \ldots < i_k \leqslant n} c_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}. \tag{8}$$

The relation (7) can be inverted and the function g_f is expressed through f as

$$g_f(\mathbf{y}) = \bigoplus_{\mathbf{x} \preccurlyeq \mathbf{y}} f(\mathbf{x}), \tag{9}$$

where $\mathbf{x} \preccurlyeq \mathbf{y}$ means that $x_k \leqslant y_k$ for $k = 1, \ldots, n$ (note that $\preccurlyeq$ is not a linear order). From this it follows that the relation $f \leftrightarrow g_f$ is one-to-one, which is referred to

as Möbius transform. It is an involution: if $g_f = h$ then $g_h = f$, or $g_{g_f} = f$ for all $f \in F_n$.

The degree $\deg f$ of a boolean function $f \in F_n$ is defined to be the maximal number d such that there is $\mathbf{y} \in V_n$ with $\mathrm{wt}(\mathbf{y}) = d$ and $g_f(\mathbf{y}) = 1$. Boolean functions of degree 1 are called affine; they can be represented as follows:

$$a(\mathbf{x}) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n = c_0 \oplus \langle \mathbf{c}, \mathbf{x} \rangle, \qquad (10)$$

where $c_0 = g_f(0, \ldots, 0)$, $c_i = g_f(0, \ldots, 1, \ldots, 0)$ (1 is on the i-th position) and $\mathbf{c} = (c_1, \ldots, c_n)$. The set of all affine functions is denoted as A_n. If $c_0 = 0$ then the affine function is called linear; such functions are denoted as l (so that $l(\mathbf{x}) = \langle \mathbf{c}, \mathbf{x} \rangle$). The set of all linear functions is denoted as L_n. It is clear that $|L_n| = 2^n$ and $|A_n| = 2^{n+1}$.

A boolean function $f \in F_n$ is called homogeneous of degree k if $g_f(\mathbf{y}) = 0$ for all $\mathbf{y} \in V_n$ with $\mathrm{wt}(\mathbf{y}) \neq k$. If, in addition, $g_f(\mathbf{y}) = 1$ for all $\mathbf{y} \in V_n$ with $\mathrm{wt}(\mathbf{y}) = k$, then f is referred to as the k-th symmetric function and denoted as s_k:

$$s_k(x_1, \ldots, x_n) = \bigoplus_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k}. \qquad (11)$$

For boolean functions one can introduce the Hemming weight and distance in the same way as it was done for boolean vectors: $\mathrm{wt}(f)$ is defined to be the number of $\mathbf{x} \in V_n$ with $f(\mathbf{x}) = 1$, and $d(f, g)$ is the number of $\mathbf{x} \in V_n$ with $f(\mathbf{x}) \neq g(\mathbf{x})$. A boolean function is called *balanced* if $\mathrm{wt}(f) = 2^{n-1}$. If we denote $f \oplus g \in F_n$ the point-wise sum of f and g,

$$(f \oplus g)(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x}), \qquad (12)$$

then $d(f, g) = \mathrm{wt}(f \oplus g)$. The distance $d(f, M)$ between a boolean function $f \in \mathcal{F}_n$ and a nonempty subset $M \subseteq \mathcal{F}_n$ is defined via

$$d(f, M) = \min_{g \in M} d(f, g). \qquad (13)$$

The distance N_f between f and A_n is called nonlinearity of f: $N_f = d(f, A_n)$. It is a very important characteristic of boolean functions.

C. Walsch-Hadamar transform

In studying properties of boolean functions the notion of Walsch-Hadamard transform can be very useful. The Walsch-Hadamard transform of a boolean function $f \in F_n$ is the integer-valued function W_f of n boolean arguments defined via

$$W_f(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x}) \oplus \langle \mathbf{x}, \mathbf{u} \rangle}. \qquad (14)$$

Let us introduce the Hadamard matrix $\tilde{H}$,

$$\tilde{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (15)$$

The tensor product $H_n = \tilde{H}^{\otimes n}$ of n copies of $\tilde{H}$ reads as

$$H_n = ((-1)^{\langle \mathbf{u}, \mathbf{v} \rangle})_{\mathbf{u}, \mathbf{v} \in V_n}. \qquad (16)$$

For any $f \in F_n$ we define two boolean vectors $\mathbf{w}_f, \mathbf{z}_f \in V_{2^n}$ via

$$\mathbf{w}_f = (W_f(\mathbf{u}))_{\mathbf{u} \in V_n}, \quad \mathbf{z}_f = ((-1)^{f(\mathbf{x})})_{\mathbf{x} \in V_n}. \qquad (17)$$

The Walsch-Hadamard transform (14) can be written in the following compact form:

$$\mathbf{w}_f = H_n \mathbf{z}_f. \qquad (18)$$

To calculate any component of $\mathbf{w}_f$ according to the definition (14) it takes $2^n - 1$ additions; to calculate all 2^n components it takes $2^n(2^n - 1) \sim 2^{2n}$additions. Using special properties of the matrix H_n, from (18) it is possible to calculate the vector $\mathbf{w}_f$ (given $\mathbf{z}_f$) with only $n2^n$ additions (fast Walsch-Hadamard transform). The algorithm and its realization in C (to be used in *Mathematica*) are described in Appendix B.

Note that all components of $\mathbf{w}_f$ are even, since a sum of an even number of equal terms is even. As an example, let us calculate $\mathbf{w}_l$ for a linear function $l(\mathbf{x}) = \langle \mathbf{c}, \mathbf{x} \rangle$. We need the following relation:

$$\sum_{\mathbf{u} \in V_n} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle} = 2^n \delta_{\mathbf{x}, \mathbf{0}}. \qquad (19)$$

This relation is obvious due to the equality

$$\sum_{\mathbf{u} \in V_n} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle} = \prod_{k=1}^{n} (1 + (-1)^{x_k}). \qquad (20)$$

Using the relation (19) from the definition (14) one can easily get

$$W_l(\mathbf{u}) = 2^n \delta_{\mathbf{u}, \mathbf{c}}, \quad \mathbf{w}_l = 2^n \mathbf{e}_{\mathbf{c}}, \qquad (21)$$

where $\mathbf{e}_{\mathbf{c}} = (0, \ldots, 1, \ldots, 0)$ (1 is on the $b_n(\mathbf{c})$-th position).

The Walch-Hadamard transform (14) is invertible; the inverse transform reads as

$$(-1)^{f(\mathbf{x})} = \frac{1}{2^n} \sum_{\mathbf{u} \in V_n} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle} W_f(\mathbf{u}), \qquad (22)$$

or, in matrix notation, as

$$\mathbf{z}_f = 2^{-n} H_n \mathbf{w}_f. \qquad (23)$$

This relation is a trivial consequence of (18) due to the simple fact that $H_n^2 = 2^n E_{2^n}$, or $H_n^{-1} = 2^{-n} H_n$. Using the same algorithm of fast Walch-Hadamard transform, one can quickly calculate $\mathbf{z}_f$ given $\mathbf{w}_f$.

Below we will need the following statement: *for an integer-valued function $W(\mathbf{u})$, $\mathbf{u} \in V_n$ there is $f \in F_n$ such that $W_f(\mathbf{u}) = W(\mathbf{u})$) if and only if $W(\mathbf{u})$ satisfies the condition*

$$\sum_{\mathbf{u} \in V_n} W(\mathbf{u}) W(\mathbf{u} \oplus \mathbf{v}) = \begin{cases} 2^{2n} & \text{if} \quad \mathbf{v} = \mathbf{0}, \\ 0 & \text{if} \quad \mathbf{v} \neq \mathbf{0}. \end{cases} \qquad (24)$$

In particular, the Walsch-Hadamar transform $W_f(\mathbf{u})$ of any boolean function $f \in F_n$ satisfies the Parseval equality:

$$\sum_{\mathbf{u}\in V_n} W_f^2(\mathbf{u}) = 2^{2n}. \tag{25}$$

The proof of this statement is quite simple. The Walsh-Hadamard transform of any boolean function $f \in \mathcal{F}_n$ satisfies the condition (24), which can be easily derived from the definition (14) using the equality (19). The less trivial part is to prove that the condition (24) is sufficient. It is enough to prove that the function

$$F(\mathbf{x}) = \frac{1}{2^n}\sum_{\mathbf{u}\in V_n}(-1)^{\langle \mathbf{x},\mathbf{u}\rangle}W(\mathbf{u}) \tag{26}$$

takes only two values ± 1. In other words, it is sufficient to prove that $F^2(\mathbf{x}) = 1$ for all $\mathbf{x} \in V_n$. We have

$$F^2(\mathbf{x}) = \frac{1}{2^{2n}}\sum_{\mathbf{u},\mathbf{v}\in V_n}(-1)^{\langle \mathbf{x},\mathbf{u}\rangle\oplus\langle \mathbf{x},\mathbf{v}\rangle}W(\mathbf{u})W(\mathbf{v}). \tag{27}$$

For any fixed $\mathbf{u} \in V_n$ the inner summation over $\mathbf{v} \in V_n$ is equivalent to the summation over $\mathbf{u} \oplus \mathbf{v}$:

$$F^2(\mathbf{x}) = \frac{1}{2^{2n}}\sum_{\mathbf{u},\mathbf{v}\in V_n}(-1)^{\langle \mathbf{x},\mathbf{v}\rangle}W(\mathbf{u})W(\mathbf{u}\oplus\mathbf{v}). \tag{28}$$

Changing the summation order we get

$$F^2(\mathbf{x}) = \frac{1}{2^{2n}}\sum_{\mathbf{v}\in V_n}(-1)^{\langle \mathbf{x},\mathbf{v}\rangle}\sum_{\mathbf{u}\in V_n}W(\mathbf{u})W(\mathbf{u}\oplus\mathbf{v}). \tag{29}$$

Due to our assumption the inner sum differs from zero only for $\mathbf{v} = \mathbf{0}$ and finally we get $F^2(\mathbf{x}) = 1$. This completes the proof.

For nonlinearity one can get the following result:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\mathbf{u}\in V_n}|W_f(\mathbf{u})|. \tag{30}$$

Let us denote $NW_f = |\{\mathbf{u} \in V_n | W_f(\mathbf{u}) \neq 0\}|$, the number of non-zero components of $\mathbf{w}_f$. Due to the Parseval equality (25) we have

$$2^{2n} = \sum_{\mathbf{u}\in V_n} W_f^2(\mathbf{u}) \leqslant NW_f \max_{\mathbf{u}\in V_n}|W_f(\mathbf{u})|^2, \tag{31}$$

and from (30) we get the inequality

$$N_f \leqslant 2^{n-1} - \frac{2^{n-1}}{\sqrt{NW_f}}. \tag{32}$$

For example, for a linear function $l \in L_n$ from (21) we have $NW_f = 1$ and from (32) it follows $N_l = 0$.

It is also possible to get an absolute upper bound for nonlinearity. According to the Parseval equality (25) we have

$$\max_{\mathbf{u}\in V_n}|W_f(\mathbf{u})| \geqslant 2^{n/2}, \tag{33}$$

and due to the relation (30) we get

$$N_f \leqslant 2^{n-1} - 2^{n/2-1}. \tag{34}$$

As we will see, for an even n this bound is exact. For an odd n the exact bound is unknown.

D. Walsh-Hadamard transform as a representation

Now another point of view on the Walsch-Hadamard transform will be presented. From the definition (14) one can easily derive the following equality:

$$\sum_{\mathbf{w}\in V_n} W_f(\mathbf{u}\oplus\mathbf{w})W_g(\mathbf{w}\oplus\mathbf{v}) = 2^n W_{f\oplus g}(\mathbf{u}\oplus\mathbf{v}), \tag{35}$$

valid for all $f, g \in F_n$. In partial case of $f = g$ it reads as

$$\sum_{\mathbf{w}\in V_n} W_f(\mathbf{u}\oplus\mathbf{w})W_f(\mathbf{w}\oplus\mathbf{v}) = 2^{2n}\delta_{\mathbf{u},\mathbf{v}}. \tag{36}$$

Let us for any $f \in F_n$ introduce the $2^n \times 2^n$-matrix W_f via

$$W_f = \frac{1}{2^n}(W_f(\mathbf{u}\oplus\mathbf{v}))_{\mathbf{u},\mathbf{v}\in V_n}. \tag{37}$$

The equality (36) means that any matrix W_f is a nontrivial root of the identity matrix: $W_f^2 = E_{2^n}$. The equality (35) means that for all $f, g \in F_n$

$$W_f W_g = W_{f\oplus g}. \tag{38}$$

In other words, the map W,

$$W : F_n \to \mathrm{GL}(\mathbf{R}^{2^n}), \quad f \to W_f, \tag{39}$$

is a representation of the additive group F_n in $\mathbf{R}^{2^n}$. Its character is given by

$$\chi(f) \equiv \mathrm{Tr}(W_f) = (-1)^{\mathrm{wt}(f)}. \tag{40}$$

Since F_n is a commutative group, W is equivalent to a direct sum of one-dimensional representations. This decomposition can be given explicitly. First, let us find eigenvalues an eigenvectors of W_f. Namely, let us show that for all $\mathbf{w} \in V_n$ the $b_n(\mathbf{w})$-th column $\mathbf{z_w}$ of H_n,

$$\mathbf{z}(\mathbf{w}) = ((-1)^{\langle \mathbf{u},\mathbf{w}\rangle})_{\mathbf{u}\in V_n}, \tag{41}$$

is an eigenvector of W_f with the corresponding eigenvalue $(-1)^{f(\mathbf{w})}$:

$$\begin{aligned}(W_f\mathbf{z}(\mathbf{w}))_{\mathbf{u}} &= \sum_{\mathbf{v}\in V_n} W_f(\mathbf{u}\oplus\mathbf{v})(-1)^{\langle \mathbf{v},\mathbf{w}\rangle} \\ &= \sum_{\mathbf{v}\in V_n}(-1)^{\langle \mathbf{u}\oplus\mathbf{v},\mathbf{w}\rangle}W_f(\mathbf{v}) \\ &= (-1)^{f(\mathbf{w})}(-1)^{\langle \mathbf{u},\mathbf{w}\rangle} = (-1)^{f(\mathbf{w})}\mathbf{z}(\mathbf{w})_{\mathbf{u}}.\end{aligned} \tag{42}$$

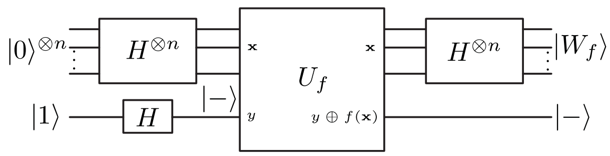


FIG. 1: Figure

This means that the matrices W_f are diagonal in the basis $\{\mathbf{z}(\mathbf{w})\}_{\mathbf{w}\in V_n}$. In particular, for the determinant of W_f we have

$$\det W_f = (-1)^{\mathrm{wt}(f)}. \tag{43}$$

The diagonalization of W_f reads as

$$W_f = 2^{-n} H_n \operatorname{diag}((-1)^{f(\mathbf{x})}_{\mathbf{x}\in V_n}) H_n. \tag{44}$$

For any fixed $\mathbf{w} \in V_n$ the map

$$f \to (-1)^{f(\mathbf{w})} \tag{45}$$

is a one-dimensional representation of F_n and the equality (44) gives the decomposition of W into the direct sum of such representations. The line spanned by $\mathbf{z}(\mathbf{w})$ is an invariant subspace of $\mathbf{R}^{2^n}$ on which W acts as (45).

E. Autocorrelation function

Another important notion is the autocorrelation function $\Delta_{f,g}(\mathbf{u})$ of two boolean functions $f, g \in F_n$, which is defined as follows:

$$\begin{aligned}\Delta_{f,g}(\mathbf{u}) &= \sum_{\mathbf{x}\in V_n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{u})} \\ &= \frac{1}{2^n}\sum_{\mathbf{v}\in V_n} (-1)^{\langle\mathbf{u},\mathbf{v}\rangle} W_f(\mathbf{v}) W_g(\mathbf{v}).\end{aligned} \tag{46}$$

Since the map $\mathbf{x} \to \mathbf{x}\oplus\mathbf{u}$ is one-to-one for a fixed $\mathbf{u}$ and idempotent, i.e. $(\mathbf{x}\oplus\mathbf{u})\oplus\mathbf{u} = \mathbf{x}$ for all $\mathbf{x}$ and $\mathbf{u}$, the autocorrelation $\Delta_{f,g}(\mathbf{u})$ is symmetric with respect to f and g: $\Delta_{f,g}(\mathbf{u}) = \Delta_{g,f}(\mathbf{u})$. For $f = g$ the autocorrelation $\Delta_{f,f}(\mathbf{u}) \equiv \Delta_f(\mathbf{u})$ is referred to as the autocorrelation of the function f.

F. Physical interpretation

Here another interpretation of Walsch-Hadamard transform is presented. Consider an n-qubit system. For any $f \in F_n$ let us introduce the state $|W_f\rangle$ via

$$|W_f\rangle = \frac{1}{2^n}\sum_{\mathbf{u}\in V_n} W_f(\mathbf{u})|\mathbf{u}\rangle. \tag{47}$$

The state $|W_f\rangle$ can be obtained using the circuit shown in Fig. 1. Here the Hadamard gate H is given by the matrix $H = 2^{-1/2}\tilde{H}$ and the $(n+1)$-gubit gate U_f acts as

$$U_f(|\mathbf{x}\rangle|y\rangle) = |\mathbf{x}\rangle|y\oplus f(\mathbf{x})\rangle. \tag{48}$$

Straightforward algebraical manipulations show that if the input state is $|0\rangle^{\otimes n}|1\rangle$ then the output state is $|W_f\rangle|-\rangle$, where

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{49}$$

Due to the Parseval equality (25) the states $|W_f\rangle$ are normalized:

$$\langle W_f|W_f\rangle = \frac{1}{2^{2n}}\sum_{\mathbf{u}\in V_n} W_f^2(\mathbf{u}) = 1, \tag{50}$$

but they are not orthogonal:

$$\langle W_f|W_g\rangle = \frac{1}{2^{2n}}\sum_{\mathbf{u}\in V_n} W_f(\mathbf{u})W_g(\mathbf{u}) = \frac{1}{2^n}\Delta_{f,g}(\mathbf{0}). \tag{51}$$

From this we can conclude: $|W_f\rangle$ and $|W_g\rangle$ are orthogonal if and only if $\Delta_{f,g}(\mathbf{0}) = 0$.

For any single-qubit operator A and for any $\mathbf{v} = (v_1, \ldots, v_n) \in V_n$ we use the notation

$$A^{\mathbf{v}} = A^{v_1} \otimes \ldots \otimes A^{v_n} \tag{52}$$

for the n-qubit factorizable gate, with k-th component to be A (if $v_k = 1$) or 1 (if $v_k = 0$). The operator with the matrix

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{53}$$

is called *NOT* gate; it acts as $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$. It is clear that for any $\mathbf{v} \in V_n$

$$X^{\mathbf{v}}|\mathbf{u}\rangle = |\mathbf{u}\oplus\mathbf{v}\rangle. \tag{54}$$

From the equality (24) we have

$$\langle W_f|X^{\mathbf{v}}|W_f\rangle = \frac{1}{2^{2n}}\sum_{\mathbf{u}\in V_n} W_f(\mathbf{u})W_f(\mathbf{u}\oplus\mathbf{v}) = \delta_{\mathbf{v},\mathbf{0}}, \tag{55}$$

i.e. all diagonal matrix elements of the from $\langle W_f|X^{\mathbf{v}}|W_f\rangle$ of any non-trivial operator (with $\mathbf{v} \neq \mathbf{0}$) operator $X^{\mathbf{v}}$ are equal to zero.

Let us also consider the phase gate

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{56}$$

It acts as $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$. It is clear that

$$Z^{\mathbf{v}}|\mathbf{u}\rangle = (-1)^{\langle\mathbf{u},\mathbf{v}\rangle}|\mathbf{u}\rangle. \tag{57}$$

There is a generalization of the equality (51):

$$\langle W_f|Z^{\mathbf{v}}|W_g\rangle = \frac{1}{2^n}\Delta_{f,g}(\mathbf{v}), \tag{58}$$

valid for all $\mathbf{v} \in V_n$.

For any state $|W_f\rangle$ let us consider 2^n states

$$X^{\mathbf{v}}|W_f\rangle = \frac{1}{2^n}\sum_{\mathbf{u}\in V_n} W_f(\mathbf{u}\oplus\mathbf{v})|\mathbf{u}\rangle. \tag{59}$$

Below it will be shown that

$$X^{\mathbf{v}}|W_f\rangle = |W_{f_{\mathbf{v}}}\rangle, \tag{60}$$

where $f_{\mathbf{v}}(\mathbf{x}) = f(\mathbf{x}) \oplus \langle\mathbf{x},\mathbf{v}\rangle$. Due to the relation (51) the states $|W_{f_{\mathbf{v}}}\rangle$ and $|W_{f_{\mathbf{w}}}\rangle$ with different $\mathbf{v}$ and $\mathbf{w}$ are orthogonal:

$$\langle W_{f_{\mathbf{v}}}|W_{f_{\mathbf{w}}}\rangle = \delta_{\mathbf{v},\mathbf{w}}. \tag{61}$$

One can easily prove that for all $\mathbf{v} \in V_n$

$$\sum_{\mathbf{u}\in V_n} W_f(\mathbf{u}\oplus\mathbf{v}) = \sum_{\mathbf{u}\in V_n} W_f(\mathbf{u}) = (-1)^{f(\mathbf{0})}2^n, \tag{62}$$

from which we get the following relation

$$\sum_{\mathbf{v}\in V_n} |W_{f_{\mathbf{v}}}\rangle = (-1)^{f(\mathbf{0})}\sum_{\mathbf{u}\in V_n}|\mathbf{u}\rangle. \tag{63}$$

Since the matrix W_f is non-degenerate according to (43), for any fixed $f \in \mathcal{F}_n$ the 2^n vectors $|W_{f_{\mathbf{v}}}\rangle$, $\mathbf{v} \in V_n$ form a basis of the state space of n qubits. The equality (63) shows that the sum of the new basic vectors (the diagonal of the parallelepiped spanned by the new basic vectors) is modulo the sign equal to the old one.

G. Uncertainty relation

Let $N\Delta_f$ be the number of $\mathbf{u} \in V_n$ with $\Delta_f(\mathbf{u}) \neq 0$. Then the following statement is valid [12]: *for all $f \in F_n$ the numbers NW_f and $N\Delta_f$ satisfy the inequality*

$$NW_f N\Delta_f \geqslant 2^n. \tag{64}$$

The quantity $U(f) \geqslant 1$, defined via

$$U(f) = \frac{1}{2^n}NW_f N\Delta_f, \tag{65}$$

is referred to as the uncertainty of $f \in F_n$.

In cryptographical applications of boolean functions theory the numbers NW_f and $N\Delta_f$ play an important role. In some applications it is necessary to use boolean functions f with small NW_f, in others with small $N\Delta_f$. The inequality (64) shows that both the numbers NW_f and $N\Delta_f$ cannot be small, they are subject to (64). In this sense the inequality (64) can be called the uncertainty relation for boolean functions.

$f(x_1,x_2)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$B_2(f)$	(i,j)
0	0	0	0	0	1	$(1,1)$
$(1+x_1)(1+x_2)$	1	0	0	0	2	$(1,2)$
$x_2+x_1x_2$	0	1	0	0	3	$(1,3)$
x_2	1	1	0	0	4	$(1,4)$
$x_1+x_1x_2$	0	0	1	0	5	$(2,1)$
x_1	1	0	1	0	6	$(2,2)$
x_1+x_2	0	1	1	0	7	$(2,3)$
$1+x_1x_2$	1	1	1	0	8	$(2,4)$
x_1x_2	0	0	0	1	9	$(3,1)$
$1+x_1+x_2$	1	0	0	1	10	$(3,2)$
$1+x_1$	0	1	0	1	11	$(3,3)$
$1+x_1+x_1x_2$	1	1	0	1	12	$(3,4)$
$1+x_2$	0	0	1	1	13	$(4,1)$
$1+x_2+x_1x_2$	1	0	1	1	14	$(4,2)$
$x_1+x_2+x_1x_2$	0	1	1	1	15	$(4,3)$
1	1	1	1	1	16	$(4,4)$

TABLE II: Boolean function visualization for $n = 2$.

H. Visualization of boolean functions

Now an approach to the visualization of the set of boolean functions will be presented. The set F_n can be identified with the set $\mathcal{B}_{2^n}$ using the map b_n (remember (2) and (6)):

$$B_n = b_{2^n} : F_n \ni f \to \sum_{\mathbf{x}\in V_n} f(\mathbf{x})2^{b_n(\mathbf{x})} \in \mathcal{B}_{2^n}. \tag{66}$$

Then with each function $f \in F_n$ one can associate a pair of integers (i,j) such that

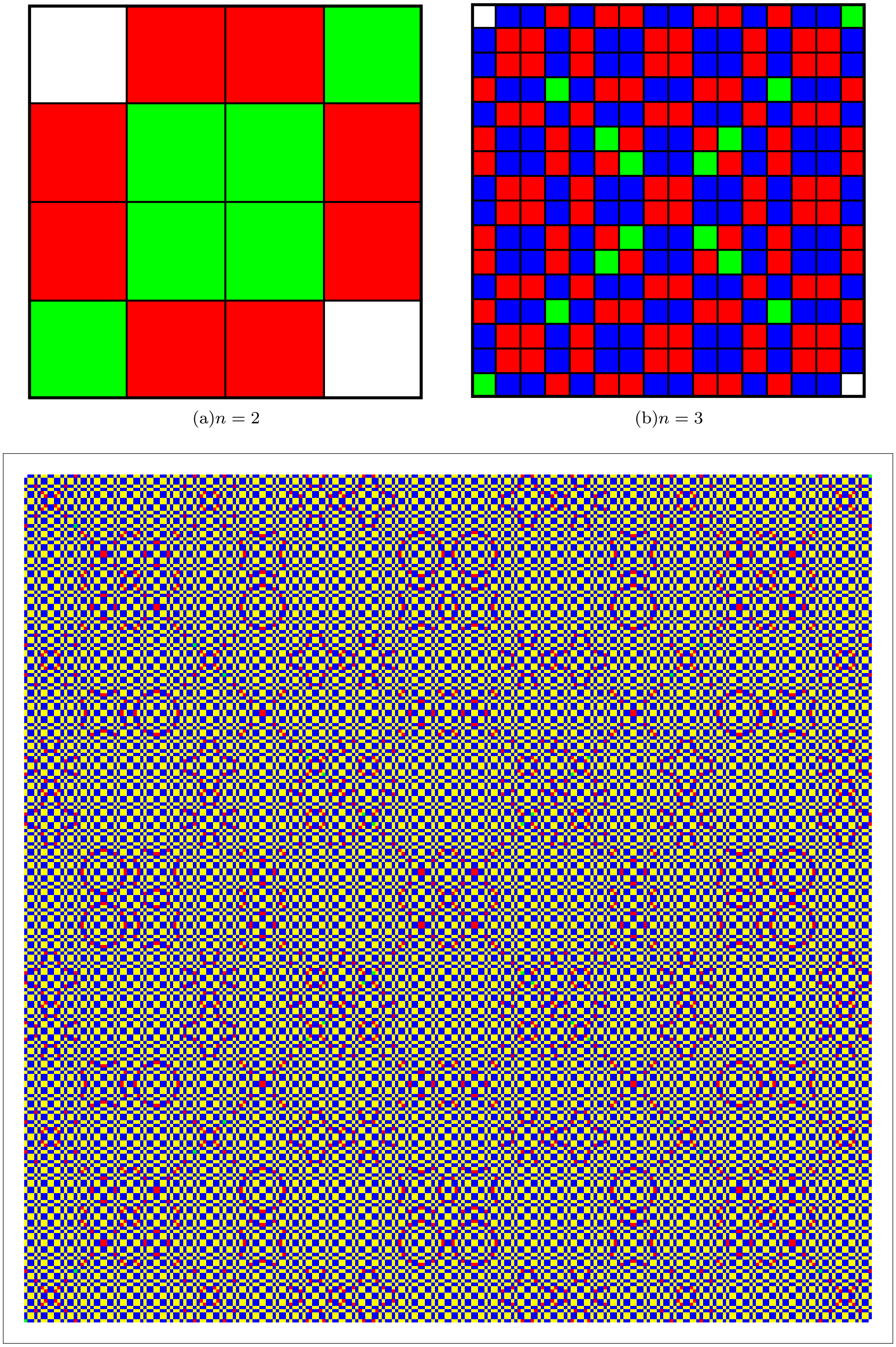
$$B_n(f) = (i-1)2^{2^{n-1}} + (j-1). \tag{67}$$

When f varies over $\mathcal{F}_n$, the corresponding pair (i,j) runs over the square

$$\mathrm{Sq}_n = \{(i,j)|1 \leqslant i,j \leqslant 2^{2^{n-1}}\}. \tag{68}$$

As an example, the correspondence between $f \in F_2$ and Sq_2 is shown in the Table II. This square can be depicted as a $2^{2^{n-1}} \times 2^{2^{n-1}}$ array of cells, with each cell marked with a definite color. For example, one can mark the cells corresponding to the functions of the same degree with the same color. Below we present pictures of F_n colored with respect to different characteristics of boolean functions, not only degree.

Let us start with the visualization of boolean functions of different orders. In Fig. 2 the cases of $n = 2$, $n = 3$ and $n = 4$ are shown. Each subfigure contains $n + 1$ different colors. Then let us visualize boolean functions in the three cases with respect to the uncertainty $U(f)$, (65). Fig. 3 shows the same three cases of $n = 2$, $n = 3$ and $n = 4$.

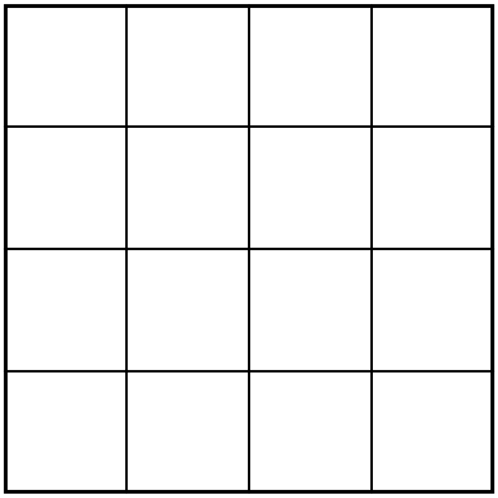


(a)$n = 2$

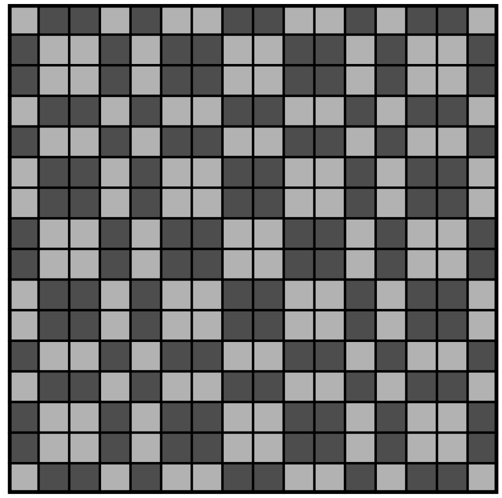
(b)$n = 3$

(c)$n = 4$

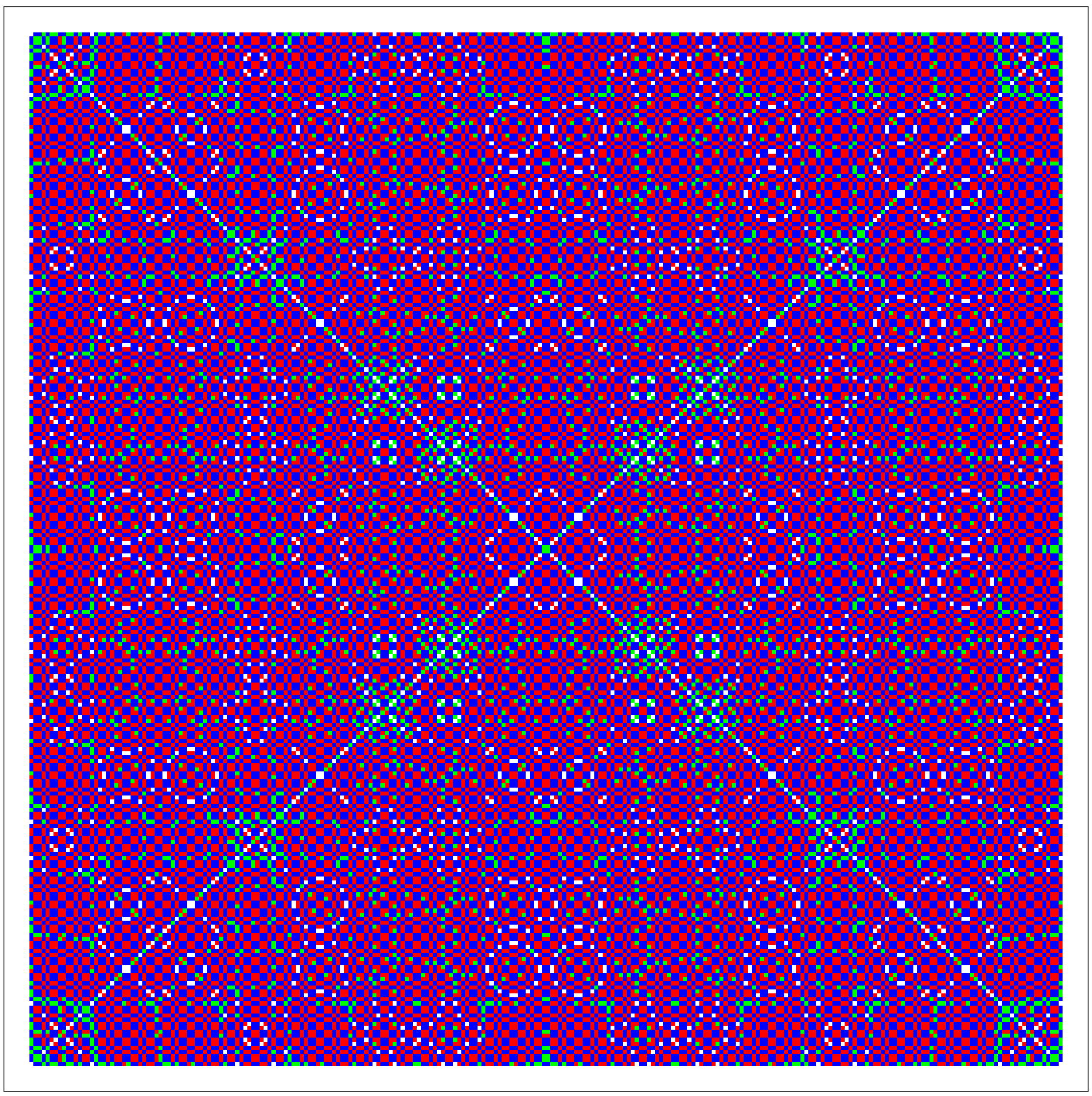
FIG. 2: Boolean functions of different orders. White corresponds to the zero order (constant) functions, green to the first order, red to the second order, yellow to the third order and blue to the forth order functions.



(a)$n = 2$. White corresponds to $U(f) = 1$.



(b)$n = 3$. Light gray corresponds to $U(f) = 1$, black to 8.



(c)$n = 4$. White corresponds to $U(f) = 1$, yellow to 35/8, red to 8 and blue to 16.

FIG. 3: Uncertainties for three different cases.

III. BELL INEQUALITIES

In this section the Bell inequalities for n qubits and especially the extremal subclass of Mermin inequalities are considered and the relation between the maximal violation of a given Bell inequality and the nonlinearity of the corresponding boolean function is discussed.

A. Construction of Bell inequalities

Consider n pairs of random variables $A_i(0)$, $A_i(1)$, $i = 1, \dots, n$ taking only two values ± 1. Let $E(\mathbf{u})$, $\mathbf{u} = (u_1, \dots, u_n) \in V_n$ be the mathematical expectation of the product of n variables $A_i(u_i)$, $i = 1, \dots, n$:

$$E(\mathbf{u}) = \mathbf{M}(A_1(u_1) \dots A_n(u_n)). \tag{69}$$

Clearly, all 2^n expectations $E(\mathbf{u})$, $\mathbf{u} \in V_n$, satisfy the inequality

$$|E(\mathbf{u})| \leqslant 1. \tag{70}$$

Can any 2^n numbers $E(\mathbf{u})$ subject to (70) be the mathematical expectations according to (69)? The answer is negative.

Let us illustrate this statement by a simple example in the case of $n = 2$. For $E(u_1, u_2)$ we have

$$E(u_1, u_2) = 2\mathbf{P}(A_1(u_1) = A_2(u_2)) - 1. \tag{71}$$

From this expression one can conclude that

$$E(u_1, u_2) = 1 \Leftrightarrow \mathbf{P}(A_1(u_1) = A_2(u_2)) = 1, \tag{72}$$

and that

$$E(u_1, u_2) = -1 \Leftrightarrow \mathbf{P}(A_1(u_1) = A_2(u_2)) = 0. \tag{73}$$

It is easy to see that the numbers $(1, 1, 1, -1)$ cannot be the expectations $(E(0,0), E(0,1), E(1,0), E(1,1))$. In fact, from (72) for $(u_1, u_2) = (0,0)$, $(0,1)$ and $(1,0)$ it follows that in such a case for any realization of $A_1(0)$, $A_1(1)$, $A_2(0)$ and $A_2(1)$ we would have $A_1(1) = A_2(0) = A_1(0) = A_2(1)$, but from (73) for $(u_1, u_2) = (1,1)$ we would have $A_1(1) \neq A_2(1)$. This contradiction proves that the numbers $(1, 1, 1, -1)$ cannot be the expectations (69).

Now a set of necessary and sufficient conditions for $E(\mathbf{u})$, $\mathbf{u} \in V_n$ to be the expectations (69) is derived. These conditions were obtained in [9]. Our approach follows the idea of [14]. For a fixed $f \in F_n$ consider the random variable A_f defined via

$$A_f = \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x})} \prod_{i=1}^{n} (A_i(0) + (-1)^{x_i} A_i(1)). \tag{74}$$

For any realization of $A_i(u_i)$ the product in (74) differs from zero only for one $\mathbf{x} \in V_n$, and for this $\mathbf{x}$ the product is equal to $\pm 2^n$; for all other $2^n - 1$ boolean vectors $\mathbf{x} \in V_n$ it equals to zero. We see that for any $f \in F_n$ only one term in the sum (74) differs from zero and equals to $\pm 2^n$ so that the sum takes only two values $\pm 2^n$. From this one can conclude that

$$|\mathbf{M}(A_f)| \leqslant 2^n. \tag{75}$$

The random variable A_f can be written in the following form:

$$\begin{aligned} A_f &= \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x})} \sum_{\mathbf{u} \in V_n} (-1)^{(\mathbf{x}, \mathbf{u})} A_1(u_1) \dots A_n(u_n) \\ &= \sum_{\mathbf{u} \in V_n} W_f(\mathbf{u}) A_1(u_1) \dots A_n(u_n). \end{aligned} \tag{76}$$

Taking the mathematical expectation, the inequality (75) becomes

$$\left| \sum_{\mathbf{u} \in V_n} W_f(\mathbf{u}) E(\mathbf{u}) \right| \leqslant 2^n. \tag{77}$$

Note that for the function $\overline{f}(\mathbf{x}) = 1 \oplus f(\mathbf{x})$ we have $W_{\overline{f}}(\mathbf{u}) = -W_f(\mathbf{u})$, and due to this the inequality (77) for $f \in F_n$ is equivalent to two inequalities

$$\sum_{\mathbf{u} \in V_n} W_f(\mathbf{u}) E(\mathbf{u}) \leqslant 2^n \tag{78}$$

for f and $\overline{f}$. The 2^{2^n} inequalities (78) for $f \in F_n$ are referred to as Bell inequalities. They form a necessary and sufficient condition for $E(\mathbf{u})$ to be the mathematical expectations (69).

Note that the inequality (70) is equivalent to two inequalities

$$E(\mathbf{u}) \leqslant 1 \quad \text{and} \quad -E(\mathbf{u}) \leqslant 1. \tag{79}$$

The first inequality is the Bell inequality (78) with the linear function $f(\mathbf{x}) \equiv l(\mathbf{x}) = \langle \mathbf{u}, \mathbf{x} \rangle$; the second one corresponds to the affine function $\overline{l}(\mathbf{x}) = 1 \oplus \langle \mathbf{u}, \mathbf{x} \rangle$, so the trivial inequalities (70) are Bell inequalities with affine functions.

The Bell inequalities (78) can be written in the following formal form:

$$\langle W_f | E \rangle \leqslant 1, \tag{80}$$

where $|E\rangle$ is a (non-normalized) state defined via

$$|E\rangle = \sum_{\mathbf{u} \in V_n} E(\mathbf{u}) |\mathbf{u}\rangle. \tag{81}$$

If $A_i(u_i)$, $i = 1, \dots, n$ are independent for all $u_i \in \mathbf{Z}_2$, then we have

$$E(u_1, \dots, u_n) = q_1(u_1) \dots q_n(u_n), \tag{82}$$

where $q_i(u) = 2\mathbf{P}(A_i(u) = 1) - 1$, and $|E\rangle$ is factorizable

$$|E\rangle = \bigotimes_{i=1}^{n} (q_i(0)|0\rangle + q_i(1)|1\rangle). \tag{83}$$

Since $|q_i(u)| \leqslant 1$ it is easy to check that any factorizable state (83) satisfy all the inequalities (80). But even if there are correlations between $A_i(u_i)$, their mathematical expectations (69) satisfy the Bell inequalities (78).

B. Violations of Bell inequalities

Now let $\hat{A}_i(u_i)$ be Hermitian operators (observables) with the spectra $\{-1, 1\}$ and for a given n-qubit state $\hat{\varrho}$ let $E(\mathbf{u})$ be the quantum-mechanical average

$$E(\mathbf{u}) = \langle \hat{A}_1(u_1) \dots \hat{A}_n(u_n) \rangle_{\hat{\varrho}} = \mathrm{Tr}\big(\hat{\varrho} \hat{A}_1(u_1) \dots \hat{A}_n(u_n)\big). \tag{84}$$

If we assume that for the state $\hat{\varrho}$ the result of the measurement of the observable $\hat{A}_i(u_i)$ can be described by a ±1-valued random variable $A_i(u_i)$, then the quantum mechanical average (84) equals to the mathematical expectation (69) and the quantities $E(\mathbf{u})$ defined in (84) satisfy the Bell inequalities (78). Such a state $\hat{\varrho}$ is called classically correlated. Surprisingly, there are quantum states such that the quantities (84) violate the Bell inequalities (for a definite choice of observables $\hat{A}_i(u_i)$), which means that the correlations of such states are stronger than any classical ones.

It is interesting to find out up to what extent a given Bell inequality can be violated in quantum case. In [9] it was shown that the maximal violation v_f of the Bell inequality (78) corresponding to the boolean function $f \in F_n$ reads as

$$v_f = \frac{1}{2^n} \max_{\varphi_1, \dots, \varphi_n \in [0, 2\pi]} \left| \sum_{\mathbf{u} \in V_n} e^{i(\varphi, \mathbf{u})} W_f(\mathbf{u}) \right|, \tag{85}$$

where $\varphi = (\varphi_1, \dots, \varphi_n)$ and $(\varphi, \mathbf{u}) = \sum_{k=1}^n u_k \varphi_k$. Using the definition (14) of $W_f(\mathbf{u})$, this expression can be rewritten in the following form:

$$v_f = \max_{\varphi_1, \dots, \varphi_n} \left| \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x})} \prod_{k=1}^{n} (-i)^{x_k} t_{x_k}(\varphi_k) \right|, \tag{86}$$

where $t_0(\varphi) = \cos\varphi$ and $t_1(\varphi) = \sin\varphi$. In general, it is not an easy optimization problem and the explicit form of v_f is unknown. The numerically calculated values of v_f for the small n are shown in Fig. 4. Studying the numerically obtained results one can conclude that there is no unique relation between the maximal quantum violation v_f and the nonlinearity N_f, but nevertheless the higher N_f the larger v_f (at least for $n = 2, 3, 4$). In other words, the higher nonlinearity of a boolean function function the stronger maximal quantum violation of the corresponding Bell inequality.

It was shown that the largest maximal violation reads as

$$\max_{f \in F_n} v_f = 2^{(n-1)/2}. \tag{87}$$

The inequalities on which this upper bound is attained are called Mermin inequalities [13]. In the next subsection the boolean functions corresponding to these inequalities are explicitly constructed.

C. Mermin inequalities

Let $A_i(u)$, $i = 1, \dots, n$, $u \in \mathbf{Z}_2$ be ±1-valued random variables. For $x, y \in \mathbf{Z}_2$ define the random variable $M_n(x, y)$ via

$$M_n(x, y) = \mathrm{Im} \prod_{k=1}^{n} (A_k(x) + iA_k(y)). \tag{88}$$

For an odd n the Mermin inequality reads as

$$\mathbf{M}(M_n(0, 1)) \leqslant 2^{(n-1)/2}, \tag{89}$$

and for an even n it reads as

$$\begin{aligned} \mathbf{M}\Big(&M_{n-1}(0,1)(A_n(0) + A_n(1)) \\ &+ M_{n-1}(1,0)(A_n(0) - A_n(1))\Big) \leqslant 2^{n/2}. \end{aligned} \tag{90}$$

After multiplying by a proper number, these inequalities can be written in the form (78) with $W_f(\mathbf{u}) \equiv M(\mathbf{u})$ given by

$$M(\mathbf{u}) = \begin{cases} 0 & \text{if} \quad \mathrm{wt}(\mathbf{u}) \quad \text{is even}, \\ (-1)^{\frac{\mathrm{wt}(\mathbf{u})-1}{2}} 2^{\frac{n+1}{2}} & \text{if} \quad \mathrm{wt}(\mathbf{u}) \quad \text{is odd}, \end{cases} \tag{91}$$

in the case of odd n, and by

$$M(\mathbf{u}) = \begin{cases} M(\mathbf{u}') + M(\overline{\mathbf{u}}') & u_n = 0, \\ M(\mathbf{u}') - M(\overline{\mathbf{u}}') & u_n = 1, \end{cases} \tag{92}$$

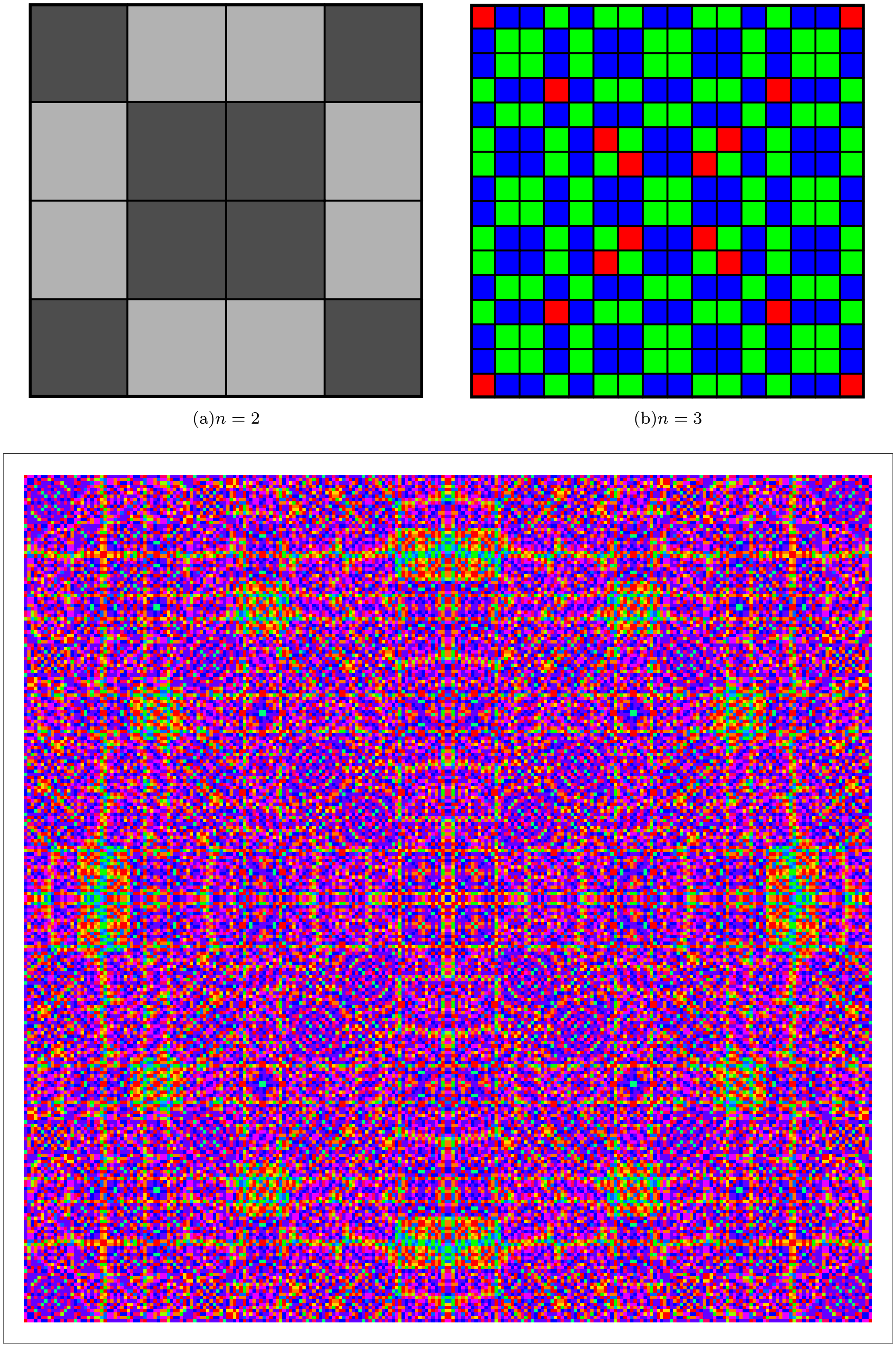
in the case of even n, where $\mathbf{u}' = (u_1, \dots, u_{n-1})$ so that $M(\mathbf{u}')$ is defined by (91).

The function $M(\mathbf{u})$ *defined by* (91) *or* (92) *satisfies the condition* (24). Let us first consider the case of odd n. For $\mathbf{v} = \mathbf{0}$ we have

$$\sum_{\mathbf{u} \in V_n} M^2(\mathbf{u}) = \sum_{\mathrm{wt}(\mathbf{u}) \text{ is odd}} 2^{n+1} = 2^{n+1} 2^{n-1} = 2^{2n}. \tag{93}$$

For $\mathbf{v} \neq \mathbf{0}$ first consider the case of odd $\mathrm{wt}(\mathbf{v})$. Then $\mathrm{wt}(\mathbf{u} \oplus \mathbf{v})$ is odd for any $\mathbf{u}$ with odd $\mathrm{wt}(\mathbf{u})$ and due to this all terms in the sum in (24) are zero and the condition (24) is satisfied. The case of even $\mathrm{wt}(\mathbf{v})$ is more difficult. If $\mathrm{wt}(\mathbf{u}) = 2m + 1$ then $M(\mathbf{u}) \sim (-1)^m$ (we omit the common factor $2^{(n+1)/2}$) and

$$\mathrm{wt}(\mathbf{u} \oplus \mathbf{v}) = \mathrm{wt}(\mathbf{u}) + \mathrm{wt}(\mathbf{v}) - 2k, \tag{94}$$



(a)$n = 2$ (b)$n = 3$

(c)$n = 4$

FIG. 4: Maximal quantum violation v_f for small n.

where $k = \mathrm{wt}(\mathbf{u}\&\mathbf{v})$. We have

$$M(\mathbf{u}\oplus\mathbf{v}) \sim (-1)^{m+\mathrm{wt}(\mathbf{v})/2-k}, \tag{95}$$

and the sum in the condition (24) reads as

$$\sum_{\mathbf{u}\in V_n} M(\mathbf{u})M(\mathbf{u}\oplus\mathbf{v}) \sim \sum_k \sum_{\mathrm{wt}(\mathbf{u}\&\mathbf{v})=k} (-1)^k. \tag{96}$$

The number of terms in the internal sum is

$$\binom{\mathrm{wt}(\mathbf{v})}{k} 2^{n-\mathrm{wt}(\mathbf{v})-1}. \tag{97}$$

According to our assumptions n is odd and $\mathrm{wt}(\mathbf{v})$ is even, hence $n-\mathrm{wt}(\mathbf{v})-1 \geqslant 0$ and the sum (96) can be calculated as

$$\sum_k \sum_{\mathrm{wt}(\mathbf{u}\&\mathbf{v})=k} (-1)^k = 2^{n-\mathrm{wt}(\mathbf{v})-1}(1-1)^{\mathrm{wt}(\mathbf{v})} = 0. \tag{98}$$

This proves that the condition (24) is satisfied also in the case of even $\mathrm{wt}(\mathbf{v})$. The case of odd n was completely considered. The proof for the case of even n easily follows from thew definition (92).

Now we will find the boolean functions which correspond to the Mermin inequalities or, in other words, which maximize v_f. First, we will find the boolean function $m \in F_n$ whose Walsch-Hadamard transform is $M(\mathbf{u})$. We start with the case of odd n. According to (22) we have

$$\begin{aligned}(-1)^{m(\mathbf{x})} &= 2^{-\frac{n-1}{2}} \sum_{\mathrm{wt}(\mathbf{u})\text{ is odd}} (-1)^{\langle\mathbf{x},\mathbf{u}\rangle+\frac{\mathrm{wt}(\mathbf{u})-1}{2}} \\ &= 2^{-\frac{n-1}{2}} \sum_{\substack{1\leqslant k\leqslant n\\ k\text{ is odd}}} (-1)^{\frac{k-1}{2}} s_k((-1)^{x_1},\ldots,(-1)^{x_n}),\end{aligned} \tag{99}$$

where s_k is the k-th symmetric polynomial

$$s_k(z_1,\ldots,z_n) = \sum_{1\leqslant i_1<\ldots<i_k\leqslant n} z_{i_1}\ldots z_{i_k}. \tag{100}$$

Note that the last sum in (99) can be written as

$$\sum_{\substack{1\leqslant k\leqslant n\\ k\text{ is odd}}} (-1)^{\frac{k-1}{2}} s_k(z_1,\ldots,z_n) = (-1)^{\frac{n+1}{2}} \operatorname{Re}\prod_{l=1}^{n}(i-z_l), \tag{101}$$

and (99) can be simplified

$$(-1)^{m(\mathbf{x})} = -(-2)^{-\frac{n-1}{2}} \operatorname{Re}\prod_{k=1}^{n}(i-(-1)^{x_k}). \tag{102}$$

Using the relation

$$i-(-1)^{x_k} = \begin{cases} -\sqrt{2}e^{-i\pi/4} & \text{if} \quad x=0, \\ \sqrt{2}e^{i\pi/4} & \text{if} \quad x=1, \end{cases} \tag{103}$$

we get the equality

$$(-1)^{m(\mathbf{x})} = (-1)^{\mathrm{wt}(\mathbf{x})-\frac{n-1}{2}} \operatorname{Re}\left((1-i)e^{i\left(\mathrm{wt}(\mathbf{x})-\frac{n-1}{2}\right)\frac{\pi}{2}}\right). \tag{104}$$

Explicitly the function $m(\mathbf{x})$ can be written as

$$m(\mathbf{x}) = \begin{cases} 0 & \text{if} \quad \mathrm{wt}(\mathbf{x})-\frac{n-1}{2} \equiv 0,3 \pmod 4, \\ 1 & \text{if} \quad \mathrm{wt}(\mathbf{x})-\frac{n-1}{2} \equiv 1,2 \pmod 4. \end{cases} \tag{105}$$

For any boolean vector $\mathbf{x} = (x_1,\ldots,x_n) \in V_n$ we have

$$\bigoplus_{k=1}^{n} x_k \equiv \mathrm{wt}(\mathbf{x}), \quad \bigoplus_{i<j} x_i x_j \equiv \binom{\mathrm{wt}(\mathbf{x})}{2} \pmod 2, \tag{106}$$

from which we get the following result:

$$m(\mathbf{x}) = \begin{cases} \bigoplus_{k=1}^{n} x_k \oplus \bigoplus_{i<j} x_i x_j & \text{if } n\equiv 1 \pmod 8, \\ \bigoplus_{i<j} x_i x_j & \text{if } n\equiv 3 \pmod 8, \\ 1\oplus \bigoplus_{k=1}^{n} x_k \oplus \bigoplus_{i<j} x_i x_j & \text{if } n\equiv 5 \pmod 8, \\ 1\oplus \bigoplus_{i<j} x_i x_j & \text{if } n\equiv 7 \pmod 8. \end{cases} \tag{107}$$

This gives the decomposition of m in the case of odd n.

In the case of even n from the definition (92) we have

$$\begin{aligned}(-1)^{m(\mathbf{x})} &= 2^{-n} \sum_{\mathbf{u}\in V_{n-1}} (-1)^{(\mathbf{x}',\mathbf{u})}(M(\mathbf{u})+M(\overline{\mathbf{u}})) \\ &+ 2^{-n} \sum_{\mathbf{u}\in V_{n-1}} (-1)^{(\mathbf{x}',\mathbf{u})+x_n}(M(\mathbf{u})-M(\overline{\mathbf{u}})),\end{aligned} \tag{108}$$

Since $n-1$ is odd, from the previous case the we can conclude that the following relations are valid:

$$\begin{aligned}\sum_{\mathbf{u}\in V_{n-1}} (-1)^{(\mathbf{x}',\mathbf{u})} M(\mathbf{u}) &= 2^{n-1}(-1)^{m(\mathbf{x}')}, \\ \sum_{\mathbf{u}\in V_{n-1}} (-1)^{(\mathbf{x}',\mathbf{u})} M(\overline{\mathbf{u}}) &= 2^{n-1}(-1)^{m(\mathbf{x}')\oplus\mathrm{wt}(\mathbf{x})\oplus x_n},\end{aligned} \tag{109}$$

from which we get

$$\begin{aligned}(-1)^{m(\mathbf{x})} &= \frac{1}{2}(-1)^{m(\mathbf{x}')} \\ &\Big(1+(-1)^{\mathrm{wt}(\mathbf{x})+x_n}+(-1)^{x_n}-(-1)^{\mathrm{wt}(\mathbf{x})}\Big),\end{aligned} \tag{110}$$

what is equivalent to the relation

$$m(\mathbf{x}) = \begin{cases} m(\mathbf{x}') & \text{if} \quad \mathrm{wt}(\mathbf{x}) \quad \text{is odd}, \\ m(\mathbf{x}')\oplus x_n & \text{if} \quad \mathrm{wt}(\mathbf{x}) \quad \text{is even}. \end{cases} \tag{111}$$

Explicitly $m(\mathbf{x})$ reads as

$$m(\mathbf{x}) = m(\mathbf{x}')\oplus\mathrm{wt}(\mathbf{x}')x_n = m(\mathbf{x}')\oplus\left(\bigoplus_{k=1}^{n-1} x_k\right)x_n. \tag{112}$$

This gives the decomposition of m in the case of even n.

We see, that in all cases $m(\mathbf{x})$ is a quadratic form and in all cases its quadratic part is the same and equals to the symmetric form s_2 (11). Below the notion for equivalence of Bell inequalities will be introduced. The maximal quantum violation v_f of equivalent Bell inequalities is the same. It was shown in [9] that all inequalities that maximize v_f are equivalent. From the considerations below we can conclude: *a boolean function $f \in F_n$ maximize v_f if and only if it is of the form*

$$f(\mathbf{x}) = a(\mathbf{x}) \oplus s_2(\mathbf{x}) = c_0 \oplus \bigoplus_{i=1}^{n} c_i x_i \oplus \bigoplus_{i<j} x_i x_j. \quad (113)$$

Affine functions correspond to the trivial Bell inequalities (79) which cannot be violated in quantum case. Adding $s_2(\mathbf{x})$ substantially changes their properties: quantum violations become the largest.

I end this subsection by showing that the boolean functions (113), which correspond to Mermin inequalities, minimize the uncertainty relation (64), i.e. $U(f) = 1$ for all functions of the form (113). Since the uncertainty is invariant under equivalence of Bell inequalities, it is sufficient to check the equality $U(f) = 1$ only for one boolean function f of the form (113). Let us take s_2. It is easy to see that

$$NW_{s_2} = \begin{cases} 2^{n-1} & \text{if } n \text{ is odd,} \\ 2^n & \text{if } n \text{ is even.} \end{cases} \quad (114)$$

Let us calculate $N\Delta_{s_2}$. We have

$$\begin{aligned} \Delta_{s_2}(\mathbf{u}) &= \sum_{\mathbf{x} \in V_n} (-1)^{\bigoplus\limits_{i<j} x_i x_j \oplus \bigoplus\limits_{i<j} (x_i \oplus u_i)(x_j \oplus u_j)} \\ &= (-1)^{\bigoplus\limits_{i<j} u_i u_j} \sum_{\mathbf{x} \in V_n} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{x} \rangle}, \end{aligned} \quad (115)$$

where $\tilde{u}_i = \bigoplus_{j \neq i} u_j$. We see that $\Delta_{s_2} \neq 0$ only if $\tilde{\mathbf{u}} = 0$, from which it follows that $u_i = \bigoplus_{i=1}^n u_i = \text{const}$. So there are at most two possibilities: $\mathbf{u} = (0, \dots, 0)$ and $\mathbf{u} = (1, \dots, 1)$. For an odd n the number $n-1$ is even and both possibilities give $\Delta_{s_2}(\mathbf{u}) = 0$, from which we have $N\Delta_{s_2} = 2$, while for an even n only the former one, $\mathbf{u} = (0, \dots, 0)$, leads to $\Delta_{s_2}(\mathbf{u}) = 0$, and in this case we have $N\Delta_{s_2} = 1$. In both cases we have $U(s_2) = 1$.

IV. CLASSIFICATION OF BELL INEQUALITIES

The number of Bell inequalities 2^{2^n} grows extremely fast with n. On the other hand, many of them are very similar, for example, differ in sign, and due to this such inequalities have similar properties (for example, they have the same maximal quantum violation). It makes sense to introduce the physically motivated notion of the equivalence of Bell inequalities and study only the classes of inequivalent inequalities.

Two Bell inequalities (and the two corresponding boolean functions) are said to be equivalent if they can be obtained from each other by applying the following three kinds of transformations (any number of times, in any order):

(i) permuting subsystems,

(ii) swapping the outcomes of any observable,

(iii) swapping the observables at any site.

Let us study these three kinds of transformations and the equivalence of Bell inequalities in more details.

A. Transformation of the first kind

The permutation of subsystems, corresponding to a permutation $\pi \in S_n$ (S_n is the symmetric group), in terms of Bell inequalities reads as: with a Bell inequality (78) corresponding to $f \in F_n$ we associate another inequality with coefficients $W_{f'}(\mathbf{u}) = W_f(\pi\mathbf{u})$, where $\pi\mathbf{u} \equiv \pi(u_1, \dots, u_n) = (u_{\pi^{-1}(1)}, \dots, u_{\pi^{-1}(n)})$. It is easy to see that the function $W_f(\pi\mathbf{u})$ satisfies the condition (24) and due to this the function f' exits. Using the inverse Walsch-Hadamard transform (22) we can find the relation between f and f':

$$\begin{aligned} (-1)^{f'(\mathbf{x})} &= \frac{1}{2^n} \sum_{\mathbf{u} \in V_n} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle} W_f(\pi\mathbf{u}) \\ &= \frac{1}{2^n} \sum_{\mathbf{u} \in V_n} (-1)^{\langle \pi\mathbf{x}, \pi\mathbf{u} \rangle} W_f(\pi\mathbf{u}) \\ &= \frac{1}{2^n} \sum_{\mathbf{u} \in V_n} (-1)^{\langle \pi\mathbf{x}, \mathbf{u} \rangle} W_f(\mathbf{u}) = (-1)^{f(\pi\mathbf{x})}. \end{aligned} \quad (116)$$

Here we used the fact that $\langle \pi\mathbf{x}, \pi\mathbf{u} \rangle = \langle \mathbf{x}, \mathbf{u} \rangle$ for all $\mathbf{x}, \mathbf{y} \in V_n$, $\pi \in \mathcal{S}_n$ and that

$$\sum_{\mathbf{u} \in V_n} F(\pi\mathbf{u}) = \sum_{\mathbf{u} \in V_n} F(\mathbf{u}). \quad (117)$$

We see that a permutation of subsystems is a permutation of the arguments of the corresponding boolean function: $f'(\mathbf{x}) = f(\pi\mathbf{x})$.

Let us define the map $p_\pi : \mathcal{F}_n \to \mathcal{F}_n$ via

$$(p_\pi f)(\mathbf{x}) = f(\pi\mathbf{x}). \quad (118)$$

Then any transformation of the type (i) is p_π for the appropriate π. Since $\pi(\sigma\mathbf{x}) = (\sigma\pi)\mathbf{x}$, we have

$$\begin{aligned} (p_\pi p_\sigma f)(\mathbf{x}) &= (p_\sigma f)(\pi\mathbf{x}) = f(\sigma(\pi\mathbf{x})) \\ &= f((\pi\sigma)\mathbf{x}) = (p_{\pi\sigma} f)(\mathbf{x}), \end{aligned} \quad (119)$$

from which we get the equality

$$p_\pi p_\sigma = p_{\pi\sigma}, \quad (120)$$

which is valid for all $\pi, \sigma \in S_n$. In other words, the map $\pi \to p_\pi$ is a representation of S_n in F_n.

In terms of the states $|W_f\rangle$ the transformation of this kind is given by the operator P_π, defined via:

$$P_\pi|\mathbf{x}\rangle = |\pi^{-1}\mathbf{x}\rangle. \tag{121}$$

It is easy to see that $W_{f'}(\mathbf{u}) = W_f(\pi\mathbf{u})$ if and only if

$$|W_{f'}\rangle = P_\pi|W_f\rangle. \tag{122}$$

This operator is nonlocal — it permutes subsystems. Note that $P_\pi P_\sigma = P_{\pi\sigma}$.

B. Transformation of the second kind

Swapping the outcomes of the observable $A_i(0)$ results in the following relations on the coefficients of Bell inequalities:

$$\begin{aligned} W_{f'}(\ldots,0,\ldots) &= -W_f(\ldots,0,\ldots), \\ W_{f'}(\ldots,1,\ldots) &= W_f(\ldots,1,\ldots). \end{aligned} \tag{123}$$

Similarly, swapping the outcomes of $A_i(1)$ we have

$$\begin{aligned} W_{f'}(\ldots,0,\ldots) &= W_f(\ldots,0,\ldots), \\ W_{f'}(\ldots,1,\ldots) &= -W_f(\ldots,1,\ldots). \end{aligned} \tag{124}$$

These relations can be written as

$$W_{f'}(\mathbf{u}) = \pm(-1)^{u_i} W_f(\mathbf{u}), \tag{125}$$

where $+$ corresponds to $A_i(1)$ and $-$ to $A_i(0)$. Swapping the outcomes of several observables $A_i(u)$ with indices $i \in I \subseteq \mathcal{N}_n = \{1,\ldots,n\}$ has the following effect:

$$W_{f'}(\mathbf{u}) = \pm(-1)^{\langle \mathbf{e}_I, \mathbf{u}\rangle} W_f(\mathbf{u}), \tag{126}$$

where all components of $\mathbf{e}_I \in V_n$ are zero except those with indices in I. Any boolean vector $\mathbf{y} \in V_n$ can be represented in the form $\mathbf{e}_I$: for any $\mathbf{y} \in V_n$ there is $I \subseteq \mathcal{N}_n$ such that $\mathbf{y} = \mathbf{e}_I$. Due to this we characterize transformations of the second kind by a boolean vector $\mathbf{y} \in V_n$, and write the relation (126) as

$$W_{f'}(\mathbf{u}) = \pm(-1)^{\langle \mathbf{y}, \mathbf{u}\rangle} W_f(\mathbf{u}). \tag{127}$$

From this it is easy to find the relation between f and f' explicitly. For the sign $+$ in (127) we have

$$(-1)^{f'(\mathbf{x})} = \frac{1}{2^n} \sum_{\mathbf{u}\in V_n} (-1)^{(\mathbf{x}\oplus\mathbf{y}, \mathbf{u})} W_f(\mathbf{u}) = (-1)^{f(\mathbf{x}\oplus\mathbf{y})}, \tag{128}$$

so that

$$f'(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{y}). \tag{129}$$

Analogously, for the sign $-$ in (127) we have

$$f'(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{y}) \oplus 1. \tag{130}$$

Let us introduce the map $\delta : F_n \to F_n$ and for any $\mathbf{y} \in V_n$ the map $s_\mathbf{y} : F_n \to F_n$ via

$$(\delta f)(\mathbf{x}) = f(\mathbf{x}) \oplus 1, \quad (s_\mathbf{y} f)(\mathbf{x}) = f(\mathbf{x}\oplus\mathbf{y}). \tag{131}$$

From the discussion above it follows that any transformation (ii) is $s_\mathbf{y}$ or $\delta s_\mathbf{y}$ for an appropriate $\mathbf{y} \in V_n$.

Consider the single qubit quantum gate with the matrix

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{132}$$

Due to the equality

$$\langle \mathbf{u}|Z^\mathbf{y}|W_f\rangle = (-1)^{\langle \mathbf{y},\mathbf{u}\rangle} W_f(\mathbf{u}) \tag{133}$$

the relations (129) and (130) are equivalent to the following ones:

$$|W_{f'}\rangle = \pm Z^\mathbf{y}|W_f\rangle. \tag{134}$$

This transformation is local.

C. Transformation of the third kind

Swapping the observables of the i-th site, $A_i(0) \leftrightarrow A_i(1)$, is expressed as

$$\begin{aligned} W_{f'}(\ldots,0,\ldots) &= W_f(\ldots,1,\ldots), \\ W_{f'}(\ldots,1,\ldots) &= W_f(\ldots,0,\ldots), \end{aligned} \tag{135}$$

or in a more compact form as

$$W_{f'}(\mathbf{u}) = W_f(\mathbf{u}\oplus\mathbf{e}_i). \tag{136}$$

Swapping the observables on several sites with indices $J \subseteq \mathcal{N}_n$ reads as

$$W_{f'}(\mathbf{u}) = W_f(\mathbf{u}\oplus\mathbf{e}_J). \tag{137}$$

As before, we characterize the transformations under study by a boolean vector $\mathbf{z} = \mathbf{e}_J$ and write the relation (137) as

$$W_{f'}(\mathbf{u}) = W_f(\mathbf{u}\oplus\mathbf{z}). \tag{138}$$

It is easy to find the relation between f and f' explicitly:

$$\begin{aligned} (-1)^{f'(\mathbf{x})} &= \frac{1}{2^n} \sum_{\mathbf{u}\in V_n} (-1)^{\langle \mathbf{x},\mathbf{u}\rangle} W_f(\mathbf{u}\oplus\mathbf{z}) \\ &= \frac{1}{2^n} \sum_{\mathbf{u}\in V_n} (-1)^{\langle \mathbf{x},\mathbf{u}\oplus\mathbf{z}} W_f(\mathbf{u}) = (-1)^{f(\mathbf{x})\oplus\langle \mathbf{x},\mathbf{z}\rangle}. \end{aligned} \tag{139}$$

For any $\mathbf{z} \in V_n$ let us introduce the map $t_\mathbf{z} : F_n \to F_n$ via

$$(t_\mathbf{z} f)(\mathbf{x}) = f(\mathbf{x}) \oplus \langle \mathbf{x},\mathbf{z}\rangle. \tag{140}$$

We see that any transformation (iii) is $t_\mathbf{z}$ for an appropriate $\mathbf{z} \in V_n$.

The relation (138) is equivalent to the following one:

$$|W_{f'}\rangle = X^\mathbf{z}|W_f\rangle. \tag{141}$$

This is also a local transform.

D. Relations between the transformations

Let us analyze relations between the maps p_π, δ, $s_{\mathbf{y}}$ and $t_{\mathbf{z}}$. It is easy to see that δ commutes with all the other maps and satisfies the relation $\delta^2 = 1$. Composition of two $s_{\mathbf{y}}$ or two $t_{\mathbf{z}}$ is again a map of the corresponding kind:

$$s_{\mathbf{y}} s_{\mathbf{y}'} = s_{\mathbf{y}\oplus\mathbf{y}'}, \quad t_{\mathbf{z}} t_{\mathbf{z}'} = t_{\mathbf{z}\oplus\mathbf{z}'}. \tag{142}$$

We see that the maps $s_{\mathbf{y}}$ form a group, isomorphic to the additive group V_n; the same is true for the maps $t_{\mathbf{z}}$.

Straightforward calculations show that the following relations are valid for all $\mathbf{y}, \mathbf{z} \in V_n$ and $\pi \in S_n$:

$$p_\pi s_{\mathbf{y}} = s_{\pi^{-1}\mathbf{y}} p_\pi, \quad p_\pi t_{\mathbf{z}} = t_{\pi^{-1}\mathbf{z}} p_\pi \tag{143}$$

Let us prove only the second relation. We have

$$(p_\pi t_{\mathbf{z}} f)(\mathbf{x}) = (t_{\mathbf{z}} f)(\pi\mathbf{x}) = f(\pi\mathbf{x}) \oplus \langle \pi\mathbf{x}, \mathbf{z}\rangle. \tag{144}$$

On the other hand, we have

$$(t_{\pi^{-1}\mathbf{z}} p_\pi f)(\mathbf{x}) = f(\pi\mathbf{x}) \oplus \langle \mathbf{x}, \pi^{-1}\mathbf{z}\rangle. \tag{145}$$

Taking into account that

$$\langle \pi\mathbf{x}, \mathbf{z}\rangle = \langle \pi^{-1}\pi\mathbf{x}, \pi^{-1}\mathbf{z}\rangle = \langle \mathbf{x}, \pi^{-1}\mathbf{z}\rangle, \tag{146}$$

we see that the last equality in (143) is valid.

The maps $s_{\mathbf{y}}$ and $t_{\mathbf{z}}$ commute modulo the map δ:

$$s_{\mathbf{y}} t_{\mathbf{z}} = \begin{cases} t_{\mathbf{z}} s_{\mathbf{y}} & \text{if} \quad \langle \mathbf{y}, \mathbf{z}\rangle = 0, \\ \delta t_{\mathbf{z}} s_{\mathbf{y}} & \text{if} \quad \langle \mathbf{y}, \mathbf{z}\rangle = 1. \end{cases} \tag{147}$$

In fact, we have

$$\begin{aligned}(s_{\mathbf{y}} t_{\mathbf{z}} f)(\mathbf{x}) &= (t_{\mathbf{z}} f)(\mathbf{x}\oplus\mathbf{y}) \\ &= f(\mathbf{x}\oplus\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{z}\rangle \oplus \langle \mathbf{y}, \mathbf{z}\rangle.\end{aligned} \tag{148}$$

Since

$$f(\mathbf{x}\oplus\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{z}\rangle = (t_{\mathbf{z}} s_{\mathbf{y}} f)(\mathbf{x}), \tag{149}$$

the equality (147) is valid.

E. The group $\mathcal{G}_n$

All the maps p_π, δ, $s_{\mathbf{y}}$ and $t_{\mathbf{z}}$ are invertible and they generate a subgroup $\mathcal{G}_n$ of the symmetric group S_{F_n} (the group of all one-to-one transformations of F_n). From the relations between p_π, δ, $s_{\mathbf{y}}$ and $t_{\mathbf{z}}$ it follows that any element $\alpha \in \mathcal{G}_n$ can be represented as

$$\alpha = \varepsilon t_{\mathbf{z}} p_\pi s_{\mathbf{y}} \tag{150}$$

in an unique way, where ε is either $\mathrm{id} : F_n \to F_n$ or δ. In particular, $|\mathcal{G}_n| = 2^{2n+1} n!$. The element α (150) acts on a function $f \in F_n$ as

$$(\alpha f)(\mathbf{x}) = \begin{cases} f(\pi\mathbf{x}\oplus\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{z}\rangle & \text{if} \quad \varepsilon = \mathrm{id}, \\ f(\pi\mathbf{x}\oplus\mathbf{y}) \oplus \langle \mathbf{x}, \mathbf{z}\rangle \oplus 1 & \text{if} \quad \varepsilon = \delta. \end{cases} \tag{151}$$

This action can be written in the following form:

$$(\alpha f)(\mathbf{x}) = f(\pi\mathbf{x}\oplus\mathbf{y}) \oplus a(\mathbf{x}), \tag{152}$$

where $a \in A_n$ is an affine function. Now we can formulate the equivalence of boolean functions (and the corresponding Bell inequalities) as follows: *two boolean functions $f, f' \in F_n$ are equivalent if there is $\alpha \in \mathcal{G}_n$ such that $f' = \alpha f$.* It is easy to see that it is really an equivalence on the set F_n. Note that $f \sim f'$ if and only if $f \oplus s_2 \sim f' \oplus s_2$ from which it follows that $S : F_n/\!\sim \to F_n/\!\sim$, $[f] \mapsto [f \oplus s_2]$ is a nontrivial involution on the set of the equivalence classes $F_n/\!\sim$. The equivalence class $[0]$ is the class of trivial inequalities and the class $S([0]) = [s_2]$ is the class of the Mermin inequalities.

The group $\mathcal{G}_n$ can be identified with the set

$$\mathcal{G}_n = \{\mathrm{id}, \delta\} \times V_n \times S_n \times V_n, \tag{153}$$

equipped with the product:

$$\begin{aligned}(\varepsilon, &\mathbf{z}, \pi, \mathbf{y})(\varepsilon', \mathbf{z}', \pi', \mathbf{y}') \\ &= (\varepsilon_0 \varepsilon \varepsilon', \mathbf{z} \oplus \pi^{-1}\mathbf{z}', \pi\pi', \pi'\mathbf{y} \oplus \mathbf{y}'),\end{aligned} \tag{154}$$

where ε_0 is defined as

$$\varepsilon_0 = \begin{cases} \mathrm{id} & \text{if} \quad \langle \mathbf{y}, \mathbf{z}'\rangle = 0, \\ \delta & \text{if} \quad \langle \mathbf{y}, \mathbf{z}'\rangle = 1. \end{cases} \tag{155}$$

The unit element e of this group is

$$e = (\mathrm{id}, \mathbf{0}, \mathrm{id}, \mathbf{0}), \tag{156}$$

where the first $\mathrm{id} : F_n \to F_n$ is the identity map on F_n and the second $\mathrm{id} : \mathcal{N}_n \to \mathcal{N}_n$ is that on $\mathcal{N}_n$. The inverse $(\varepsilon, \mathbf{z}, \pi, \mathbf{y})^{-1}$ reads as

$$(\varepsilon, \mathbf{z}, \pi, \mathbf{y})^{-1} = (\tilde{\varepsilon}\varepsilon, \pi\mathbf{z}, \pi^{-1}, \pi^{-1}\mathbf{y}), \tag{157}$$

where $\tilde{\varepsilon}$ is defined via

$$\tilde{\varepsilon} = \begin{cases} \mathrm{id} & \text{if} \quad \langle \mathbf{y}, \pi\mathbf{z}\rangle = 0, \\ \delta & \text{if} \quad \langle \mathbf{y}, \pi\mathbf{z}\rangle = 1. \end{cases} \tag{158}$$

The elements $(\varepsilon, \mathbf{z}, \mathrm{id}, \mathbf{0})$ form a normal subgroup $\mathcal{U}^{(1)}_n \lhd \mathcal{G}_n$. The elements $(\mathrm{id}, \mathbf{0}, \pi, \mathbf{y})$ form a (not normal) subgroup $\mathcal{J}_n$, usually referred to as Jevons group. The group $\mathcal{G}_n$ is the semidirect product of $\mathcal{U}^{(1)}_n$ and $\mathcal{J}_n$:

$$\mathcal{G}_n = \mathcal{U}^{(1)}_n \rtimes \mathcal{J}_n. \tag{159}$$

The elements $(\mathrm{id}, \mathbf{0}, \mathrm{id}, \mathbf{y})$ form a normal subgroup of $\mathcal{J}_n$, which is isomorphic to product of n copies of the cyclic group C_2 of second order. The elements $(\mathrm{id}, \mathbf{0}, \pi, \mathbf{0})$ form a (not normal) subgroup of $\mathcal{J}_n$ which is isomorphic to the permutation group S_n. The Jevons group $\mathcal{J}_n$ is the semidirect product of C^n_2 and S_n:

$$\mathcal{J}_n = C^n_2 \rtimes S_n, \tag{160}$$

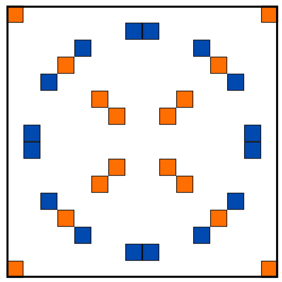
so we have the following decomposition of $\mathcal{G}_n$:

$$\mathcal{G}_n = \mathcal{U}_n^{(1)} \rightthreetimes (C_2^n \rightthreetimes S_n). \tag{161}$$

In terms of vectors $|W_f\rangle$ the equivalence can be expressed as: two boolean functions $f, f' \in \mathcal{F}_n$ are equivalent if and only if there are $\pi \in S_n$ and $\mathbf{y}, \mathbf{z} \in V_n$ such that

$$|W_{f'}\rangle = \pm P_\pi Z^{\mathbf{y}} X^{\mathbf{z}} |W_f\rangle. \tag{162}$$

This gives another interpretation of the action of the group $\mathcal{G}_n$ on the set F_n.



The classes of equivalence of Bell inequalities for small number of qubits are shown in Fig. 5. For $n = 2$ there are $N_2 = 2$ classes of equivalence, $N_3 = 5$ and $N_4 = 39$. The small squares, outlined in this figure, are shown in Fig. 6. They have the structure similar with that of the Fig. 5(b). The blue subsquares (which form a circle) correspond to Mermin inequalities, and the orange ones (which form a cross) correspond to trivial inequalities. The same picture is repeated in these subsquares, showing a kind of fractal behavior. The *Mathematica* code with which these figures were obtained is presented in the Appendix A.

The figures 5, as well as the figures 3 and 4 were obtained numerically. The analytical expressions for the number of equivalence classes and for the maximal quantum violation v_f of the equivalence class defined by a boolean function $f \in F_n$ are unknown. In the next two subsections a partial approach to this problem will be presented.

F. Pólya theory

Consider two finite sets X and Y. The notation Y^X is used for the set of all the functions $f : X \to Y$. The set Y^X is finite and has $|Y|^{|X|}$ elements, which motivates the notation. Let G be a finite group and let $\alpha : G \to S_X$ be a homomorphism of G to the symmetric group on X, i.e. an action of G on X. This means that for any $g \in G$ the map

$$\alpha_g = \alpha(g) : X \to X \tag{163}$$

is a permutation of X and the relation

$$\alpha_g \alpha_{g'} = \alpha_{gg'} \tag{164}$$

is valid for all $g, g' \in G$.

Two functions $f, f' : X \to Y$ are said to be equivalent with respect to the action α, $f \sim_\alpha f'$, if there is $g \in G$ such that $f' = f \circ \alpha_g$, i.e. if the relation

$$f'(x) = f(\alpha_g x) \tag{165}$$

is valid for all $x \in X$. What is the number N of equivalence classes? For example, if the action α is trivial, i.e. if $\alpha_g = \mathrm{id}_X$ for all $g \in G$, then $f \sim_\alpha f'$ if and only if $f = f'$, which means that each equivalence class consists of a single element and there are $|Y|^{|X|}$ equivalence classes.

To calculate the number of equivalence classes we need the notion of the cycle index of the group G. Each element $g \in G$ defines an equivalence $\sim_g$ on the set X via

$$x \sim x' \quad \text{if} \quad x' = \alpha_g(x). \tag{166}$$

Each equivalence class has the form of a cycle

$$z_g(x) = \{x, \alpha_g(x), \ldots, \alpha_g^{k(x)-1}(x)\} \tag{167}$$

of some length $k(x)$ (so that $\alpha_g^{k(x)}(x) = x$). Different cycles $z_g(x)$ do not intersect. For any fixed $g \in G$ the set X can be represented as a disjoint union of cycles

$$X = \bigcup_i z_g(x_i), \quad z_g(x_i) \cap z_g(x_j) = \varnothing \quad \text{if} \quad i \neq j. \tag{168}$$

Let $c_k(g)$ be the number of the cycles of the length k in this decomposition, $k = 1, \ldots, n = |X|$. It is clear that the numbers $c_1(g), \ldots, c_n(g)$ satisfy the following relation

$$\sum_{k=1}^{n} k c_k(g) = n. \tag{169}$$

The cycle index of G with respect to the action α is the polynomial $Z_G(x_1, \ldots, x_n)$ of n variables defined as

$$Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{c_1(g)} \ldots x_n^{c_n(g)}. \tag{170}$$

A very special case of the Pólya theorem is the following statement: *for the number of the equivalence classes (with respect to the equivalence* (165)*) we have*

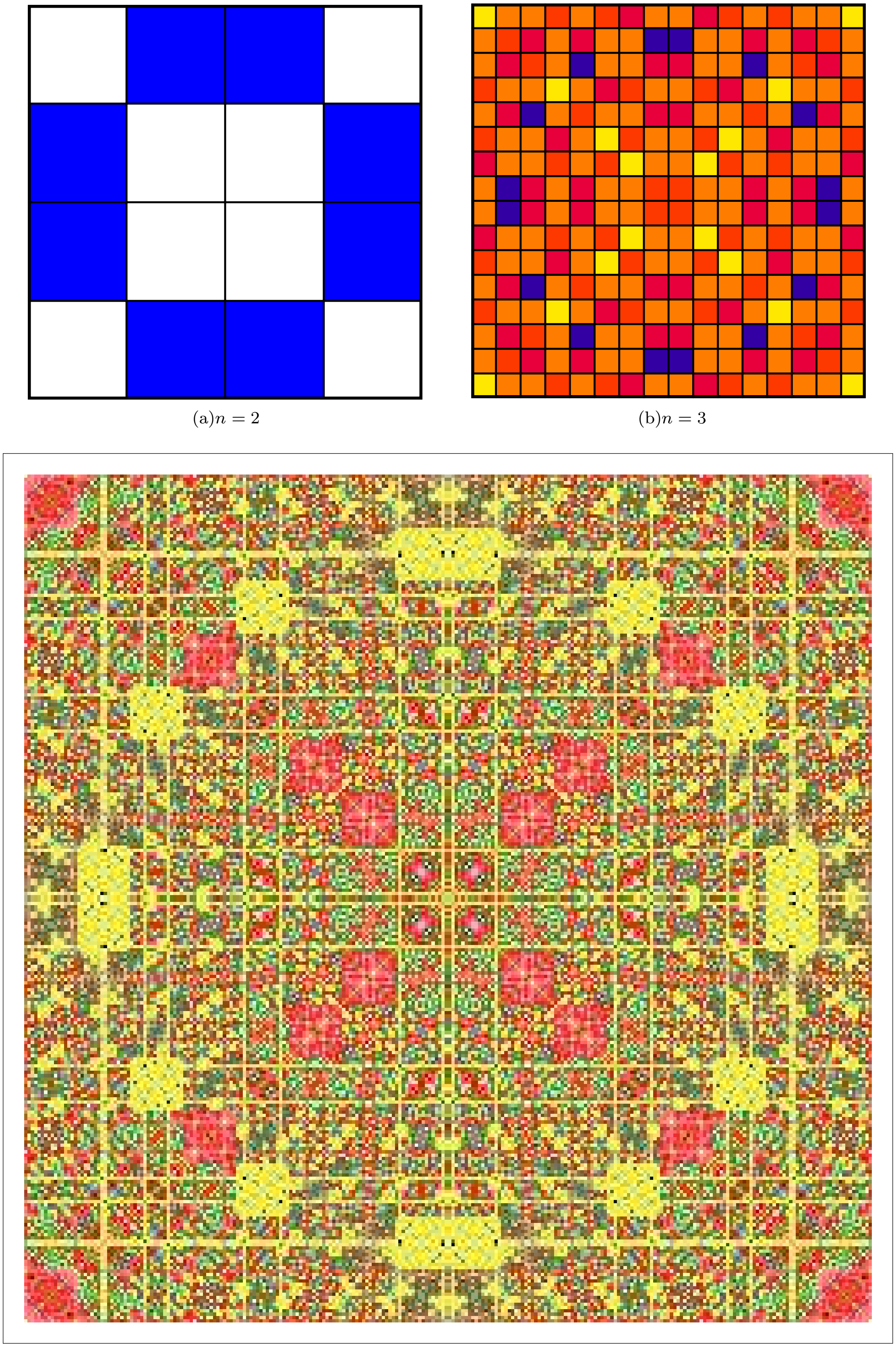
$$N = Z_G(|Y|, \ldots, |Y|). \tag{171}$$

Now consider a more general situation. where there is an action not only on X but also an action $\beta : H \to S_Y$ of the group H on Y. The equivalence of functions given by (165) can be extended as follows: $f, f' : X \to Y$ are said to be equivalent, $f \sim f'$, if there are $g \in G$ and $h \in H$ such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\alpha_g} & X \\ \big\downarrow{\scriptstyle f'} & & \big\downarrow{\scriptstyle f} \\ Y & \xrightarrow{\beta_h} & Y \end{array} \tag{172}$$

is commutative, i.e. if the relation

$$\beta_h f'(x) = f(\alpha_g x) \tag{173}$$



(a)$n = 2$ (b)$n = 3$

(c)$n = 4$

FIG. 5: The classes of equivalence of Bell inequalities for small number of qubits.

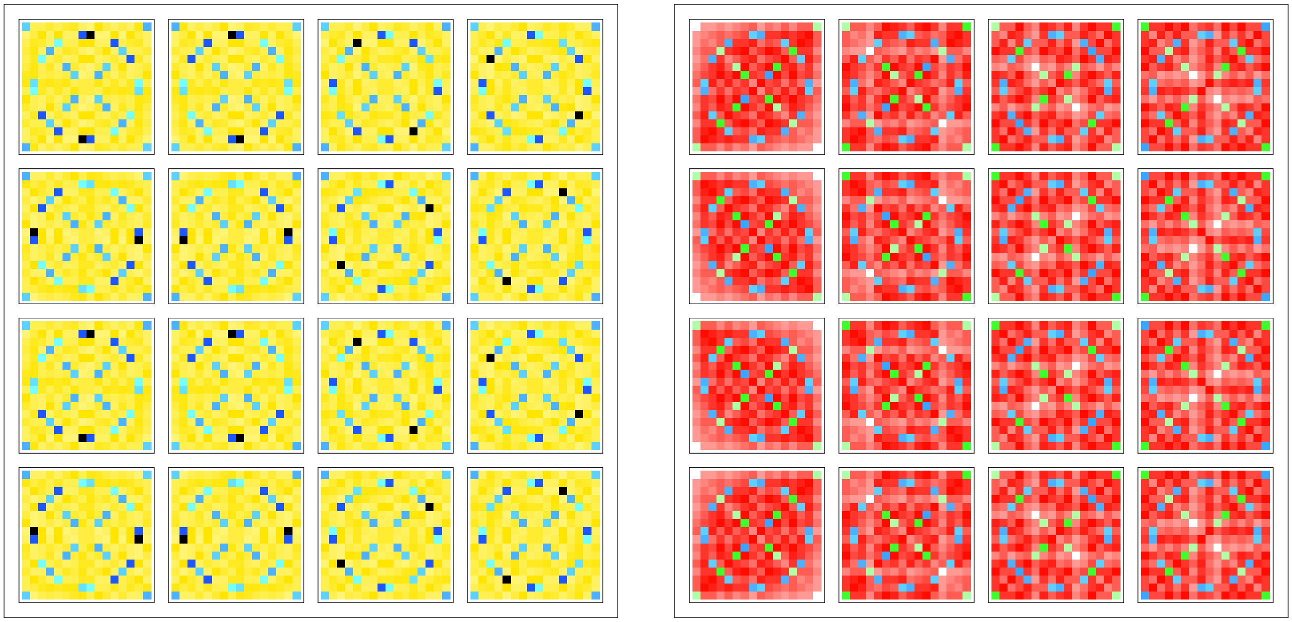


FIG. 6: The subsquares.

is valid for all $x \in X$. In this case the number N of equivalence classes can be expressed in terms of the cycle indices $Z_G(x_1, \ldots, x_n)$ and $Z_H(y_1, \ldots, y_m)$ as follows:

$$N = Z_G\left(\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_n}\right) Z_H(e^{s_1(\mathbf{z})}, \ldots, e^{m s_1(\mathbf{z})}), \quad (174)$$

where $s_1(\mathbf{z}) = \sum_{j=1}^{n} z_j$ and the derivatives are taken at $z_1 = \ldots = z_n = 0$. This expression can be transformed to another form, sometimes more suitable for calculations:

$$N = \frac{1}{|H|} \sum_{h \in H} Z_G(c_1(h), c_1(h) + 2c_2(h), \ldots), \quad (175)$$

where the i-th argument is equal to

$$\sum_{j|i} j c_j(h). \quad (176)$$

It easy to see that the previous case (where there is a action only on X) is a special case of this more general situation when the action of H on Y is trivial. In fact, in such a case we have

$$c_1(h) = |Y|, \quad c_k(h) = 0 \quad \text{if} \quad k > 1, \quad (177)$$

for all $h \in H$, and from (175) we get the relation (171):

$$N = \frac{1}{|H|} \sum_{h \in H} Z(|Y|, \ldots, |Y|) = Z(|Y|, \ldots, |Y|). \quad (178)$$

If the equivalence on the set Y^X can be represented in the form (173) then the number of equivalence classes can be calculated according to (175) (or (171)). Unfortunately, not any equivalence on Y^X can be represented in the form (173). In such cases one must find other ways to solve the problem.

G. Classification with respect Jevon's group $\mathcal{J}_n$

In our case $X = V_n$ and $Y = \mathbf{Z}_2$. The equivalence (152) cannot be represented directly in the form (173), so let us start with a simpler case. Consider the action of $\mathcal{J}_n$ on V_n, which is the reduction of the action of $\mathcal{G}_n$ to its subgroup $\mathcal{J}_n$. The cycle index of the group $\mathcal{J}_n$ was calculated in [10] and it is given by the following complicated expression:

$$Z_{\mathcal{J}_n}(x_1, \ldots, x_{2^n}) = \sum_{\mathbf{c}} \left(\frac{1}{\prod_{i=1}^{n} c_i!(2i)^{c_i}} \bigotimes_{i=1}^{n} \left(\prod_{d|i} x_d^{a(d)} + \prod_{d|2i, d\nmid i} x_d^{b(d)} \right)^{\otimes c_i} \right), \quad (179)$$

n	$Z_{\mathcal{J}_n}(x_1,\ldots,x_{2^n})$	$\overline{N}_n$	N_n
1	$\frac{1}{2}(x_1^2+x_2)$	2	1
2	$\frac{1}{8}(x_1^4+3x_2^2+2x_1^2x_2+2x_4)$	4	2
3	$\frac{1}{48}(x_1^8+13x_2^4+8x_1^2x_3^2+8x_2x_6$ $+6x_1^4x_2^2+12x_4^2)$	14	5
4	$\frac{1}{384}(x_1^{16}+51x_2^8+48x_1^2x_2x_4^3$ $+48x_8^2+12x_1^8x_2^4+84x_4^4$ $+12x_1^4x_2^6+32x_1^4x_3^4+96x_2^2x_6^2)$	222	39
5	$\frac{1}{3840}(x_1^{32}+231x_2^{16}+20x_1^{16}x_2^8$ $+520x_4^8+80x_1^8x_3^8+720x_2^4x_6^4$ $+160x_1^4x_2^2x_3^4x_6^2+320x_4^2x_{12}^2$ $+240x_1^4x_2^2x_4^6+480x_8^4+240x_2^4x_4^6$ $+60x_1^8x_2^{12}+384x_1^2x_5^6+384x_2x_{10}^3)$	616126	22442

TABLE III: Cycle index $Z_{\mathcal{G}_n}$ for small n.

where the sum is over all vectors $\mathbf{c}=(c_1,\ldots,c_n)$ with nonnegative integer components such that

$$\sum_{k=1}^{n} kc_k = n. \tag{180}$$

The function $a(k)$ is defined for any integer $k \geqslant 1$ via

$$a(k) = \frac{1}{k}\sum_{d|k} 2^d \mu\left(\frac{k}{d}\right), \tag{181}$$

and $b(2k)$ is defined for positive even integer argument $2k$, $k \geqslant 1$, via

$$b(2k) = \frac{1}{2k}\sum_{d|2k, d\nmid k} 2^{d/2} \mu\left(\frac{2k}{d}\right), \tag{182}$$

with $\mu(m)$ being the Möbius function

$$\mu(m) = \begin{cases} 1 & \text{if} \quad m=1, \\ (-1)^k & \text{if} \quad m = p_1\ldots p_k, \\ 0 & \text{in other cases,} \end{cases} \tag{183}$$

where $p_1,\ldots,p_k$ are different prime numbers.

The cross-product is defined as follows. For powers of variables we have

$$x_p^n \otimes x_q^m = x_{\mathrm{lcm}(p,q)}^{nm\,\gcd(p,q)}, \tag{184}$$

where $\gcd(p,q)$ and $\mathrm{lcm}(p,q)$ are the greatest common divisor and the least common multiple of integers p and q respectively. For two monomials the cross-product is defined via

$$(x_{p_1}^{n_1}\ldots x_{p_k}^{n_k})\otimes(x_{q_1}^{m_1}\ldots x_{q_l}^{m_l}) = \prod_{i=1}^{k}\prod_{j=1}^{l}(x_{p_i}^{n_i}\otimes x_{q_j}^{m_j}), \tag{185}$$

and then extended for arbitrary polynomials by bilinearity. For example, let us calculate the cross-product $(x_1^2x_2^3)\otimes(x_3^4x_4^5)$:

$$\begin{aligned}(x_1^2x_2^3)\otimes(x_3^4x_4^5) &= (x_1^2\otimes x_3^4)(x_1^2\otimes x_4^5)(x_2^3\otimes x_3^4)(x_2^3\otimes x_4^5) \\ &= x_3^{2\cdot 4\cdot 1}x_4^{2\cdot 5\cdot 1}x_6^{3\cdot 4\cdot 1}x_4^{3\cdot 5\cdot 2} = x_3^8x_4^{40}x_6^{12}.\end{aligned} \tag{186}$$

The cycle index $Z_{\mathcal{J}_n}$ for small n is shown in the second column of the table III.

Now let us add an action on the set $Y=\mathbf{Z}_2$. Let $H=C_2=\{1,\tau\}$ be the cyclic group of the second order. The action β we define as: $\beta_1=\mathrm{id}_{\mathbf{Z}_2}$ and β_τ being the logical *NOT*, $\beta_\tau(0)=1$ and $\beta_\tau(1)=0$. For cycle lengthes we have

$$c_1(1)=2, \quad c_2(1)=0, \quad c_1(\tau)=0, \quad c_2(\tau)=1. \tag{187}$$

According to (175) for the number of equivalence classes we have the following expression (see also [11]):

$$\overline{N}_n = \frac{1}{2}\Big(Z_G(2,\ldots,2)+Z_G(0,2,0,2,\ldots)\Big). \tag{188}$$

These numbers are shown in the third column of the table III. The last column of the table shows the number N_n of equivalence classes with respect to the equivalence under study. The number N_5 was taken from *www.ii.uib.no/ larsed/boolean/*. The numbers N_n for $n>5$ are unknown.

V. CONCLUSION

In conclusion, the relation between the boolean functions theory and the general Bell inequalities for n-qubits is established. The classification of Bell inequalities with respect to the Jevons group is obtained, which is a weaker result then the problem posed in [9]. Nevertheless, to my knowledge it is the only approach to the more general classification. This approach is based on the works [10, 11] done for computer logic circuits theory, which shows the connection between quite different problems — qubit system description and computer logic circuit design.

There are still many unsolved problems. Two the most important ones are:

(i) classification of Bell inequalities (or boolean functions) with respect to the group $\mathcal{G}_n$,

(ii) characterization of the maximal quantum violation v_f of a given boolean function f in terms of properties of f, in particular, finding the relation between v_f and the nonlinearity N_f.

And, of course, a very interesting question — how the ideas from different applications of the boolean functions theory (not only to cryptography or computer logic circuits design) can be used in quantum information theory.

APPENDIX A: THE CODE

In this Appendix I present the *Mathematica* code Figs. 2, 3, 4, 5 and Table III were obtained with. First of all, the set V_n can be coded as

```
In[1]:=  V[n_] := Tuples[{0,1},n]
```
(A1)

The *Mathematica* function IntegerDigits[n, b, l] gives the list of the base-b digits of n, padding it on the left if necessary to give a list of length l. Using this function, one can code V_n in another way as

```
V[n_] := IntegerDigits[#,2,n]&/@Range[0,2^n - 1]
```

This code works a few times more slowly, but this approach can be useful if it necessary to construct only some part of V_n, not the whole set V_n. We know that $F_n \simeq V_{2^n}$, but since $2^{2^6} > 10^{19}$, the simple definition `F[n_] := V[2^n]` will not work for $n \geqslant 6$.

A general boolean function (8) can be coded as follows:

```
In[2]:=  f[c_,S_] := Function[x,Mod[c.(Apply[Times,#]&/@ (Part[x,#]&/@ S)),2]]
```
(A2)

where `J` is the list of all the multi-indices $(i_1,\dots,i_k)$ for which the coefficients $c_{i_1,\dots,i_k} \neq 0$ and `c` the list of these coefficients. Note that the `Length`-es of `c` and `J` must be the same. For example, the expression

```
f[c,Subsets[Range[n],{m}]]
```
(A3)

gives a homogeneous polynomial of the degree m (except the case when all elements of `c` are zero; when all elements of the list `c` are 1 then (A3) is the m-th symmetric polynomial (11):

```
f[Table[1,{Binomial[n,m]}],Subsets[Range[n],{m}]][{x1,...,xn}] = sm(x1,...,xn)
```
(A4)

Similarly, the expression

```
f[c,Subsets[Range[n],m]]
```
(A5)

is a polynomial of the degree not greater then m.

The Walsch-Hadamard transform can be coded as

```
In[3]:=  WHT := Function[u,Plus @@ (Function[x,(-1)^(#[x]+(x.u))]/@ V[Length[u]])]&
```
(A6)

This method of calculation the Walsch-Hadamard transform is very simple and quite ineffective. In Appendix B a much better method is presented. The only disadvantage of that method is the fact that it works much faster only when it is necessary to calculate all the numbers $W_f(\mathbf{u})$, $\mathbf{u} \in V_n$ simultaneously, and it cannot be applied to calculate only one number $W_f(\mathbf{u})$ for a given $\mathbf{u} \in V_n$. `WHT` is a functional: `WHT[f]` is a function and `WHT[f][{u1,...,un}]` is its value $W_f(\mathbf{u})$ at $\mathbf{u} = (u_1,\dots,u_n)$. The inverse Walsch-Hadamard transform can be coded as

```
In[4]:=  WHIT := Function[x,(1 - 2^(-Length[x]) Plus @@ (Function[u,(-1)^(x.u) #[u]]/@ V[Length[x]]))/2]&
```
(A7)

Like WHT, it is also a functional.

The autocorrelation (46) of two boolean functions can be coded as

$$In[5]{:=}\quad \mathtt{\Delta := Function[u, Plus @@ (Function[x, (-1)^{\#1[x]+\#2[Mod[\#,2]\&/@ (x+u)]}]/@ V[Length[u]])]\&} \tag{A8}$$

It is a functional of two arguments: the expression $\mathtt{\Delta[f,g][\{u_1,\ldots,u_n\}]}$ is the value $\Delta_{f,g}(\mathbf{u})$ at $\mathbf{u} = (u_1,\ldots,u_n)$.

The uncertainty (65) can be coded as

$$In[6]{:=}\quad \mathtt{U[n\_] := Function[f, 2^{-n}Count[WHT[f]/@ V[n], \_?(\#! = 0\&)]Count[\Delta[f,f]/@ V[n], \_?(\#! = 0\&)]]} \tag{A9}$$

For a function $f \in F_n$ the expression U[n][f] gives the uncertainty $U(f)$ of f. To calculate $U(f)$ for all $f \in F_n$ we need a way to define f given its number $B_n(f)$, $0 \leqslant B_n(f) < 2^{2^n}$. The following code solves this problem:

$$In[7]{:=}\quad \mathtt{itof[n\_, B\_] := Part[IntegerDigits[B, 2, 2^n], 2^n - FromDigits[\#, 2]]\&} \tag{A10}$$

Given $0 \leqslant B < 2^{2^n}$, the expression itof[n,B] is the corresponding boolean function, to which one can apply the syntaxis $\mathtt{itof[n,B][\{x_1,\ldots,x_n\}]}$. We can visualize boolean functions with respect to their uncertainty using the code

$$In[8]{:=}\quad \mathtt{ut[n\_] := Partition[Table[U[n][itof[n,B]], \{B, 0, 2^{2^n} - 1\}], 2^{2^{n-1}}]} \tag{A11}$$

In *Mathematica* this table can be immediately plotted with the ArrayPlot function, what was doe for the case of $n = 4$, for the other two cases I used a simple script to generate *pstricks* code from this table and then compiled it with LaTeX(*pstricks* code produced huge pictures in the case of $n = 4$). In this way Fig. 3 was obtained. The code

$$\mathtt{ut[n]//Flatten//Sort//Split//Length} \tag{A12}$$

gives the number of different values of the uncertainty. For $n = 2$ it is 1 (all 16 boolean functions have the same uncertainty 1), for $n = 3$ it is 2 (the values are 1 and 8) and for $n = 4$ it is 4 (the values are 1, 35/8, 8 and 16). Unfortunately, these are all the values of n for which this simple code works, for larger n another technique is needed.

Now I will show how the Fig. 2 was obtained. The key point is the function

$$\begin{aligned} In[9]{:=}\quad & \mathtt{d[n\_, m\_] := Function[c, FromDigits[f[c, Subsets[Range[n], m]]/@ V[n], 2]]} \\ & \mathtt{/@ V[Plus @@ (Binomial[n, \#]\&/@ Range[0, m])]} \end{aligned} \tag{A13}$$

which returns the numbers $B_n(f)$ of the boolean functions $f \in F_n$ of degree $\leqslant m$. To visualize boolean func-

tions with respect to their degree let us create a list $\mathtt{dt} = \mathtt{Table}[\mathtt{n}, \{2^{2^{\mathtt{n}}}\}];$. Then we can fill it in as

$$\mathtt{For}[\mathtt{i} = 1, \mathtt{i} \leqslant \mathtt{n}, \mathtt{i} + +, \mathtt{dt}[[\mathtt{d}[\mathtt{n}, \mathtt{n} - \mathtt{i}] + 1]] = \mathtt{n} - \mathtt{i}] \tag{A14}$$

The table $\mathtt{Partition}[\mathtt{dt}, 2^{2^{\mathtt{n}-1}}]$ gives the desired visualization.

Now let us discuss the equivalence of Bell inequalities. The map p_π (118) can be coded as

$$In[10]{:=}\quad \mathtt{p}[\mathtt{pi\_}] := \mathtt{Function}[\mathtt{x}, \#[\mathtt{Permute}[\mathtt{x}, \mathtt{InversePermutation}[\mathtt{pi}]]]]\& \tag{A15}$$

The expression $\mathtt{p}[\mathtt{pi}]$ is a functional: $\mathtt{p}[\mathtt{pi}][\mathtt{f}]$ gives the function $p_\pi f$, and $\mathtt{p}[\mathtt{pi}][\mathtt{f}][\{\mathtt{x_1}, \dots, \mathtt{x_n}\}]$ gives its value $(p_\pi f)(\mathbf{x})$ at $\mathbf{x} = (x_1, \dots, x_n)$. The maps δ, $s_{\mathbf{y}}$ (131) and $t_{\mathbf{z}}$ (140) can be coded as

$$\begin{aligned} &In[11]{:=}\quad \delta := \mathtt{Function}[\mathtt{x}, 1 - \#[\mathtt{x}]]\& \\ &In[12]{:=}\quad \mathtt{s}[\mathtt{y\_}] := \mathtt{Function}[\mathtt{x}, \#[\mathtt{Function}[\mathtt{z}, \mathtt{Mod}[\mathtt{z}, 2]]/@\ (\mathtt{x} + \mathtt{y})]]\& \\ &In[13]{:=}\quad \mathtt{t}[\mathtt{z\_}] := \mathtt{Function}[\mathtt{x}, \mathtt{Mod}[\#[\mathtt{x}] + \mathtt{x.z}, 2]]\& \end{aligned} \tag{A16}$$

Let us illustrate the relations between the maps under study. As an example, consider the first relation (143). I show that this relation is valid by applying the maps from both sides to all boolean functions $f \in F_n$ and comparing the results. To do it, we need operations which produce the lists of values $\{(p_\pi s_{\mathbf{y}} f)(\mathbf{x})\}$ and $\{(s_{\mathbf{y}} p_\pi f)(\mathbf{x})\}$, $\mathbf{x} \in V_n$ given the list $\{f(\mathbf{x})\}$, $\mathbf{x} \in V_n$ of values of $f \in F_n$. The code

$$\begin{aligned} &In[14]{:=}\quad \mathtt{ps}[\mathtt{n\_}, \mathtt{pi\_}, \mathtt{y\_}] := \mathtt{Composition}[\mathtt{p}[\mathtt{pi}], \mathtt{s}[\mathtt{y}]][\mathtt{Function}[\mathtt{x}, \mathtt{Part}[\#, \mathtt{FromDigits}[\mathtt{x}, 2] + 1]]]/@\ \mathtt{V}[\mathtt{n}]\& \\ &In[15]{:=}\quad \mathtt{sp}[\mathtt{n\_}, \mathtt{pi\_}, \mathtt{y\_}] := \mathtt{Composition}[\mathtt{s}[\mathtt{y}], \mathtt{p}[\mathtt{pi}]][\mathtt{Function}[\mathtt{x}, \mathtt{Part}[\#, \mathtt{FromDigits}[\mathtt{x}, 2] + 1]]]/@\ \mathtt{V}[\mathtt{n}]\& \end{aligned} \tag{A17}$$

is a solution to this problem. The expression

$$In[16]{:=}\quad \mathtt{ps}[3, \{2, 3, 1\}, \{1, 1, 0\}]/@\ \mathtt{V}[2^3] - \mathtt{sp}[3, \{2, 3, 1\}, \{1, 0, 1\}]/@\ \mathtt{V}[2^3]//\mathtt{Short} \tag{A18}$$

produces a list of zero-lists, as expected. This example clearly demonstrates that the first relation (143) is valid (in the case of $n = 3$).

$$\begin{aligned} &\{\{0, 0, 0, 0, 0, 0, 0, 0\}, << 254 >>, \\ &\{0, 0, 0, 0, 0, 0, 0, 0\}\} \end{aligned} \tag{A19}$$

Given a number $0 \leqslant B < 2^{2^n}$ the function

$$\begin{aligned}
&\mathit{In}[17]{:=}\quad \mathtt{e[n_,B_]\ :=\ Replace[FromDigits[Map[\#,V[n]],2]\&}\\
&\qquad \mathtt{/@\ Function[f,Apply[Function[\{\varepsilon,y,pi,z\},Composition[\varepsilon,t[z],p[pi],s[y]]}\\
&\qquad \mathtt{[Function[x,Part[IntegerDigits[f,2,2^n],FromDigits[x,2]+1]]]],\#]\&}\\
&\qquad \mathtt{/@\ Tuples[\{\{Identity,\delta\},V[n],Permutations[Range[n]],V[n]\}]][B]}\\
&\qquad \mathtt{//Sort//Split,\{(i_)..\}\to i,1]}
\end{aligned} \tag{A20}$$

produces the list of numbers which correspond to the functions, equivalent to the one corresponding to B. With this functions it is easy to get the equivalence classes. Let us illustrate the general idea by the case of $n = 3$. We start with $B = 0$: `e[3,0]//Short` produces

$$\{0,15,51,<<10>>,204,240,255\} \tag{A21}$$

It is the first class of equivalence (which contains 16 elements). The smallest number which is not in this class is 1; `e[3,1]//Short` produces

$$\{1,2,4,<<122>>,251,253,254\} \tag{A22}$$

It is the second class of equivalence (which contains 128 elements). The smallest number which is not in either class found so far is 3; `e[3,3]//Short` produces

$$\{3,5,10,<<42>>,245,250,252\} \tag{A23}$$

It is the third class of equivalence (which contains 48 elements). The ext number to try is 6: `e[3,6]//Short` produces

$$\{6,9,18,<<42>>,237,246,249\} \tag{A24}$$

It is the fourth class of equivalence (which also contains 48 elements). The next number is 23; `e[3,23]//Short` produces

$$\{23,24,36,<<10>>,219,231,232\} \tag{A25}$$

it is the fifth class of equivalence (which contains 16 elements). Since $16+128+48+48+16 = 256$, we exhausted all numbers (boolean functions) which means that in the case of $n = 3$ there are 5 classes of equivalence, they are shown in Fig. 5(b). The same approach allows one to get Fig. 5(c).

The maximal quantum violations can be found as follows. Let us introduce the functions

$$\begin{aligned}
&\mathit{In}[18]{:=}\quad \mathtt{S[\varphi_]\ :=\ \{Cos[\varphi],I\ Sin[\varphi]\}}\\
&\mathit{In}[19]{:=}\quad \mathtt{S[\varphi_List]\ :=\ Apply[Times,\#]\&}\\
&\qquad\qquad \mathtt{/@\ Tuples[S/@\ \varphi]}
\end{aligned} \tag{A26}$$

The maximal violation (86) can now be coded as

$$\begin{aligned}
&\mathit{In}[20]{:=}\quad \mathtt{v[f_,\varphi_]\ :=\ Abs[((-1)^{f[\#]}\&}\\
&\qquad\qquad \mathtt{/@\ V[Length[\varphi]]).S[\varphi]]}\\
&\mathit{In}[21]{:=}\quad \mathtt{v2[B_,\varphi_]\ :=\ v[itof[Length[\varphi],B],\varphi]}
\end{aligned} \tag{A27}$$

The quantity $\mathtt{v2[B,\varphi]}$ give the maximal quantum violation v_f of the function f corresponding to the number B. Let us illustrate the calculation of maximal quantum violation for Mermin inequalities. The Mermin inequalities (whose coefficients are given by (91) and (92)) can be coded as (using the standard package *Algebra‘SymmetricPolynomials*)

$$\mathtt{m[x\_]\ :=\ Mod[SymmetricPolynomial[x,2],2]} \tag{A28}$$

The maximal quantum violation of Mermin inequalities can be found as

$$\begin{aligned}
&\mathit{In}[22]{:=}\quad \mathtt{FindMaximum[v[m,\{\varphi_1,\ldots,\varphi_n\}],}\\
&\qquad\qquad \mathtt{\{\varphi_1,\varphi_1^0\},\ldots,\{\varphi_n,\varphi_n^0\}]}
\end{aligned} \tag{A29}$$

For example, the code

$$\mathtt{FindMaximum[v[m,\{\varphi_1,\varphi_2\}],\{\varphi_1,1\},\{\varphi_2,1\}]} \tag{A30}$$

produces

$$\{1.41421,\{\varphi_1\to\ 0.785398,\varphi_2\to\ 0.785398\}\} \tag{A31}$$

the code

$$\begin{aligned}
&\mathtt{FindMaximum[v[m,\{\varphi_1,\varphi_2,\varphi_3\}],}\\
&\mathtt{\{\varphi_1,1\},\{\varphi_2,1\},\{\varphi_3,1\}]}
\end{aligned} \tag{A32}$$

produces

$$\{2.,\{\varphi_1\to\ 0.785398,\varphi_2\to\ 0.785398,\varphi_3\to\ \ldots\}\} \tag{A33}$$

in full agreement with the relation (87). Since v_f is the same for equivalent functions, using the classes of equivalence calculated before, it is easy to get Fig. 4.

Now I will show how the table III was obtained. To calculate the cycle index $Z_{\mathcal{J}_n}(x_1,\ldots,x_{2^n})$ we need to calculate the sum (179). The vectors $\mathbf{c}$ for a given n can be obtained using the standard package *Combinatorica*, containing the function `Partitions[n]`, which returns the list of partitions of n. Any partition p of this list has the following form

$$p = \{\underbrace{n_1,\ldots,n_1}_{k_1},\underbrace{n_2,\ldots,n_2}_{k_2},n_3,\ldots\}, \tag{A34}$$

with $n_1 > n_2 > n_3 > \ldots$ and $k_1 n_1 + k_2 n_2 + \ldots = n$. The relation

$$p \to \mathbf{c} = \{\underbrace{\overbrace{\ldots,k_2}^{n_2},\ldots,k_1}_{n_1},\ldots\} \tag{A35}$$

gives a one-to-one correspondence between the partitions of n and the vectors $\mathbf{c}$. Here k_i is on n_i-th place and the other components are zero. This correspondence can be realized in *Mathematica* via

$$\begin{aligned}
&In[23]{:=}\quad \mathtt{ct[p_] := Module[\{c = Table[0, \{Plus\ @@\ p\}]\},}\\
&\qquad\qquad \mathtt{Set[Part[c, \#[[1]]], Length[\#]]\&/@\ Split[p];}\\
&\qquad\qquad \mathtt{Return[c]}\\
&\qquad\quad \mathtt{]}
\end{aligned} \tag{A36}$$

Then we need to define the cross-product. We introduce the object $\mathtt{var[p, n]}$ which represents the n-th power of the p-th independent variable. The code

$$In[24]{:=}\quad \mathtt{cp[var[p\_, n\_], var[q\_, m\_]]\ :=\ var[LCM[p, q], n\ m\ GCD[p, q]]} \tag{A37}$$

reproduces the definition (184). To extend the cross-product for arbitrary polynomials we need the following definitions (the order in which they are given is important):

$$\begin{aligned}
&In[25]{:=}\quad \mathtt{cp[v_, c_] := c\ v/;\ NumericQ[c]}\\
&In[26]{:=}\quad \mathtt{cp[c_, v_] := c\ v/;\ NumericQ[c]}\\
&In[27]{:=}\quad \mathtt{cp[v1_ + v2_, v3_] := cp[v1, v3] + cp[v2, v3]}\\
&In[28]{:=}\quad \mathtt{cp[v3_, v1_ + v2_] := cp[v3, v1] + cp[v3, v2]}\\
&In[29]{:=}\quad \mathtt{cp[v3_, v1_v2_] := cp[v3, v1]\ cp[v3, v2]}\\
&In[30]{:=}\quad \mathtt{cp[v1_v2_, v3_] := cp[v1, v3]\ cp[v2, v3]}\\
&In[31]{:=}\quad \mathtt{cp[c_v1_, v2_] := c\ cp[v1, v2]/;\ NumericQ[c]}\\
&In[32]{:=}\quad \mathtt{cp[v1_, c_v2_] := c\ cp[v1, v2]/;\ NumericQ[c]}
\end{aligned} \tag{A38}$$

The following code reproduces the identities $(x_p^n)^m = x_p^{nm}$ and $x_p^n x_p^m = x_p^{n+m}$ respectively:

$$\begin{aligned}
&In[33]{:=}\quad \mathtt{var/:\ Power[var[p_, n_], m_]\ :=\ var[p, n\ m]}\\
&In[34]{:=}\quad \mathtt{var/:\ var[p_, n_]\ var[p_, m_]\ :=\ var[p, n + m]}
\end{aligned} \tag{A39}$$

The code for the functions a (181) and b (182) is obvious:

$$\begin{aligned}
&In[35]{:=}\quad \mathtt{a[k_]\ :=\ \frac{1}{k}Plus\ @@\ \left(2^{\#}\ MoebiusMu\left[\frac{k}{\#}\right]\&/@\ Divisors[k]\right)}\\
&In[36]{:=}\quad \mathtt{b[k_]\ :=\ \frac{1}{k}Plus\ @@\ \left(2^{\#/2}MoebiusMu\left[\frac{k}{\#}\right]\&/@\ Complement[Divisors[k],\ Divisors[k/2]]\right)}
\end{aligned} \tag{A40}$$

A factor of of the sum (179) can be coded as

```
In[37]:=  factor[i_] := Times @@ (var[#, a[#]]&/@ Divisors[i]) + Times @@ (var[#, b[#]]&
              /@ Complement[Divisors[2i], Divisors[i]])                                   (A41)
```

A term of the sum is coded as

```
In[38]:=  term[c_] := Module[{t},
            t = MapIndexed[If[#1 == 0, 1, If[#1 == 1, factor[#2[[1]]],
              Fold[cp, factor[#2[[1]]], Table[factor[#2[[1]]], {#1 - 1}]]]]&, c];      (A42)
            Fold[cp, First[t], Rest[t]]
          ]/(Times @@ (Factorial/@ c)Times @@ MapIndexed[(2#2[[1]])^#1&, c])
```

The whole sum (179) is given by

```
In[39]:=  cycleIndex[n_] := Plus @@ (term/@ (ct/@ Partitions[n]))                        (A43)
```

The number $\overline{N}_n$ can be obtained as follows:

```
In[40]:=  ub[n_] := 1/2((cycleIndex[n] /. {var[p_, k_] -> 2^k})
            +(cycleIndex[n] /. {var[p_, k_] :> If[EvenQ[p], 2^k, 0]}))                     (A44)
```

Then one can get the numbers form the table III: the code `Table[ub[n], {n, 1, 5}]` produces {2, 4, 14, 222, 616126}.

APPENDIX B: FAST WALSCH-HADAMARD TRANSFORM

A much faster way of calculating the Walsch-Hadamar transform of a boolean function $f \in F_n$ (i.e. calculation of all 2^n numbers $W_f(\mathbf{u})$, $\mathbf{u} \in V_n$) is based on the following decomposition of the Hadamard matrix:

$$H_n = \prod_{k=1}^{n} M_{n-k+1} \equiv \prod_{k=1}^{n} (E_{n-k} \otimes H \otimes E_{k-1}), \tag{B1}$$

which can be proved by induction. The relation $\mathbf{y} = M_k\mathbf{x}$ can be written as

$$\begin{aligned} y_{j2^k+i} &= x_{j2^k+i} + x_{j2^k+2^{k-1}+i}, \\ y_{j2^k+2^{k-1}+i} &= x_{j2^k+i} - x_{j2^k+2^{k-1}+i}, \end{aligned} \tag{B2}$$

for $i = 1, \ldots, 2^{k-1}$ and $j = 0, \ldots, 2^{n-k} - 1$. The Walsh-Hadamard transform can be calculated according to (18) as

$$\mathbf{w}_f = M_n \ldots M_1 \mathbf{z}_f. \tag{B3}$$

Starting with the vector $\mathbf{x} = \mathbf{z}_f$ we calculate vectors $\mathbf{y}_k = M_k \ldots M_1 \mathbf{z}_f$ for $k = 1, \ldots, n$. Then $\mathbf{y}_n$ is $\mathbf{w}_f$. The algorithm in C is presented in the function *whtl* in the file *whtl.c* below. To turn *whtl.c* into a program usable from inside *Mathematica* another file, *whtl.tm* is necessary.

whtl.tm

```
:Begin:
:Function:            whtl
:Pattern:             WHTL[x_List]
:Arguments:           {x}
:ArgumentTypes:       {IntegerList}
:ReturnType:          Manual
:End:
```

whtl.c

```c
#include "mathlink.h"
#include <stdlib.h>
#include <string.h>

// xlen is of the form 2^n, returns n
long __log(long xlen) {
  long i = 1, m = xlen;
  while((m >>= 1) != 1) i++;
  return i;
}

void whtl(int *x, long xlen) {
  int *y = (int*)calloc(xlen, sizeof(int));
  long i, j, k, t, pow1, pow2, ind1, ind2;
  long n = __log(xlen);

  for(k = 1; k <= n; k++) {
    pow1 = 1<<(k-1);
    pow2 = 1<<(n-k);
    for(j = 0; j < pow2; j++) {
      t = j<<k;
      // in C arrays are numbered from 0
      for(i = 0; i < pow1; i++) {
        ind1 = t + i;
        ind2 = ind1 + pow1;
        y[ind1] = x[ind1] + x[ind2];
        y[ind2] = x[ind1] - x[ind2];
      }
    }
    if(k < n)
      memcpy(x, y, sizeof(int)*xlen);
  }

  MLPutIntegerList(stdlink, y, xlen);
  free(y);
}

int main(int argc, char* argv[]) {
  return MLMain(argc, argv);
}
```

On a UNIX system the files are compiled with the following command

$$\texttt{\$ mcc -o WHTL whtl.tm whtl.c} \tag{B4}$$

This command produces an executable file *WHTL*. To use it in *Mathematica* it must be installed as

$$\texttt{Install["/path/to/program/WHTL"];} \tag{B5}$$

Then it can be used as

$$\texttt{WHTL}[\{z_1, \ldots, z_{2^n}\}] \tag{B6}$$

where all z_i, $i = 1, \ldots, 2^n$ are ± 1.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] N. Bohr, Phys. Rev. **48**, 696 (1935).
[3] J. S. Bell, Physics **1**, 195 (1964).
[4] A. Aspect, G. Roger, S. Reynaud, J. Dalibard, and C. Cohen-Tannoudji, Phys. Rev. Lett. **45**, 617 (1980).
[5] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
[6] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982).
[7] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).
[8] A. Aspect, Nature **398**, 189 (1999).
[9] R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001).
[10] M. Harrison, University of Michigan Technical Note **04879-3-T** (1962).
[11] M. Harrison, University of Michigan Technical Note **04879-4-T** (1962).
[12] O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, *Boolean functions in coding theory and cryptography* (MCNMO, Moscow, 2004).
[13] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[14] G. Schachner, quant-ph/0312117.